

	GLOBAL DECISION SUPPORT SYSTEM (GDSS) APPLICATION SUPPORT SERVICES
Organization:	HQ AMC C2 SYSTEMS BRANCH (HQ AMC/A6IM)
Address:	203 W Losey St, Scott AFB, IL 62225

Performance Work Statement

8 June 2017

1. Description of Services

1.1 Background

The Global Decision Support System (GDSS) is maintained/sustained by the United States Air Force (USAF), Headquarters (HQ) Air Mobility Command (AMC). In 2011, GDSS replaced multiple legacy systems with a single enhanced system; a modernized, fully integrated Command and Control (C2) decision support system using open systems infrastructure and shared relational database. GDSS supports the Defense Transportation System and Distribution Process Owner migration strategies. GDSS is designed around a client-server environment composed of web applications, server processes, Commercial Off-the-Shelf (COTS) relational database management system, database schema, and supporting utility scripts. GDSS is a United States Transportation Command (USTRANSCOM)-funded, Mission Assurance Category (MAC) level one, National Security System (NSS) system. It is the Mobility Air Forces (MAF) premiere C2 system within USTRANSCOM's Defense Transportation System (DTS) providing world-wide, near real-time data to combatant commanders throughout the full spectrum of military operations. As the MAF's principal C2 system, GDSS is the execution authority for mission management, providing robust capabilities in a net-centric environment, and allowing access and information sharing across unclassified and classified domains using continuous multi-master replicated databases. GDSS interoperates with Air Force, Army, and Joint C2 systems, and interfaces with other key Department of Defense (DOD), USTRANSCOM, Joint and AMC C2 and transportation management systems while utilizing the USTRANSCOM Distributed Enclave architecture. GDSS is an extension of the USTRANSCOM network providing a full computing infrastructure to include network, servers, security and storage. Replication is provided using four near real-time replicated unclassified and classified C2 enclaves for redundancy and performance. Currently, there are over 20,000 active user accounts from 261 major sites world-wide. GDSS user demographics include aircrew, airfield managers, C2 controllers, flight managers, intelligence, maintenance, mission planners, stage managers, transportation managers, and weather. GDSS directly draws and/or pushes data to the following systems: Advanced Computer Flight Planning System, Virtual Threat Assessor, Single Mobility System, TRANSCOM Reference Data Management, AF Aircraft Maintenance System-GO81, Aviation Resource Management System, 618 AOC Data and Web Services, Weather Data Analysis system, Air National Guard, Cargo Movement Operations System, DEAMS Consolidated Billing System, 15/17 Operational Weather Squadron, and Global Combat Support System; and also interfaces with 18 additional systems through the Mobility Enterprise Information System.

Aviation Operational Risk Management (AvORM) is a component application of GDSS. The AvORM system provides integration of manual and automated analysis applications for AMC mission planning and execution, C2 systems. The AvORM analysis system includes human factors such as planning and scheduling tools to optimize aircrew utilization and enhance AMC military aviation operations.

AMC's Services Oriented Architecture (SOA) and data foundational construct resides within the Mobility Enterprise Information Services (MEIS3). The MEIS3 environment is a collection of defined information/application services, running on a flexible hardware environment, exposing AMC's C2/Total Asset Visibility (TAV) information to external/internal consumers. The services enhance data sharing, information sharing, and orchestrate event-driven activities. The MEIS3 provides the functional air operations and Joint

Deployment and Distribution Enterprise information, data, and status in a form defined by the appropriate AMC functional communities to enhance decision-making and planning processes of the Combatant Commanders, Combined Force Air Component Commander, Joint Force Air Component Commander, Director of Mobility Forces and their staffs. AMC's SOA foundation (i.e. MEIS3) is directly tied to AMC's transportation business processes leveraging open architecture, adaptive environment, loosely-coupled components, real web-applications (Web 2.0), and, in the near future, secure mobile-accessible applications. MEIS3 will be phased out as MEIS4 capabilities are fielded.

Additionally, USTRANSCOM has directed the migration of GDSS to a Cloud environment.

1.2 Mission and Organization

AMC/A6's mission is to provide integrated Command, Control, Communications, and Computer Information (C4I) systems and manage strategic C4I resources in support of AMC's global air mobility mission. At the highest level, GDSS users are mission operators from the military services, Department of Defense (DOD), and other Federal agencies. The capabilities required in the Command and Control of the Mobility Air Forces (MAF) include: Deploy and Distribute, Understand, Plan, Decide, Direct, and Execute. GDSS ties together these capabilities with the warfighter.

The GDSS Program of Record (POR) includes the following applications: GDSS (Core), AvORM, MEIS 3/MGOP, MCS, EMC, MSD, GDSS Training Suites, GDSS Exercise Suites, and Prototype Suites. Within this document these applications will be referred to as GDSS unless otherwise stated.

1.3 The following diagram illustrates the current interfaces that give GDSS a formidable and dynamic command and control capability; Situational awareness from strategic to finite details; Ability to direct or re-direct forces with accuracy, current data, integration with Air Traffic Control (ATC), weather, and in real or near real time.

The Contractor shall be required to understand these system relationships during the Phase-in (90 days after contract award); the nature of each interface in terms of the data it pulls, pushes or gets from and/or to GDSS and the purpose of that data, as well as a comprehensive technical understanding of each interface connected to GDSS. Figure 1-2 is for informational purposes only and subject to change as interfaces are modified.

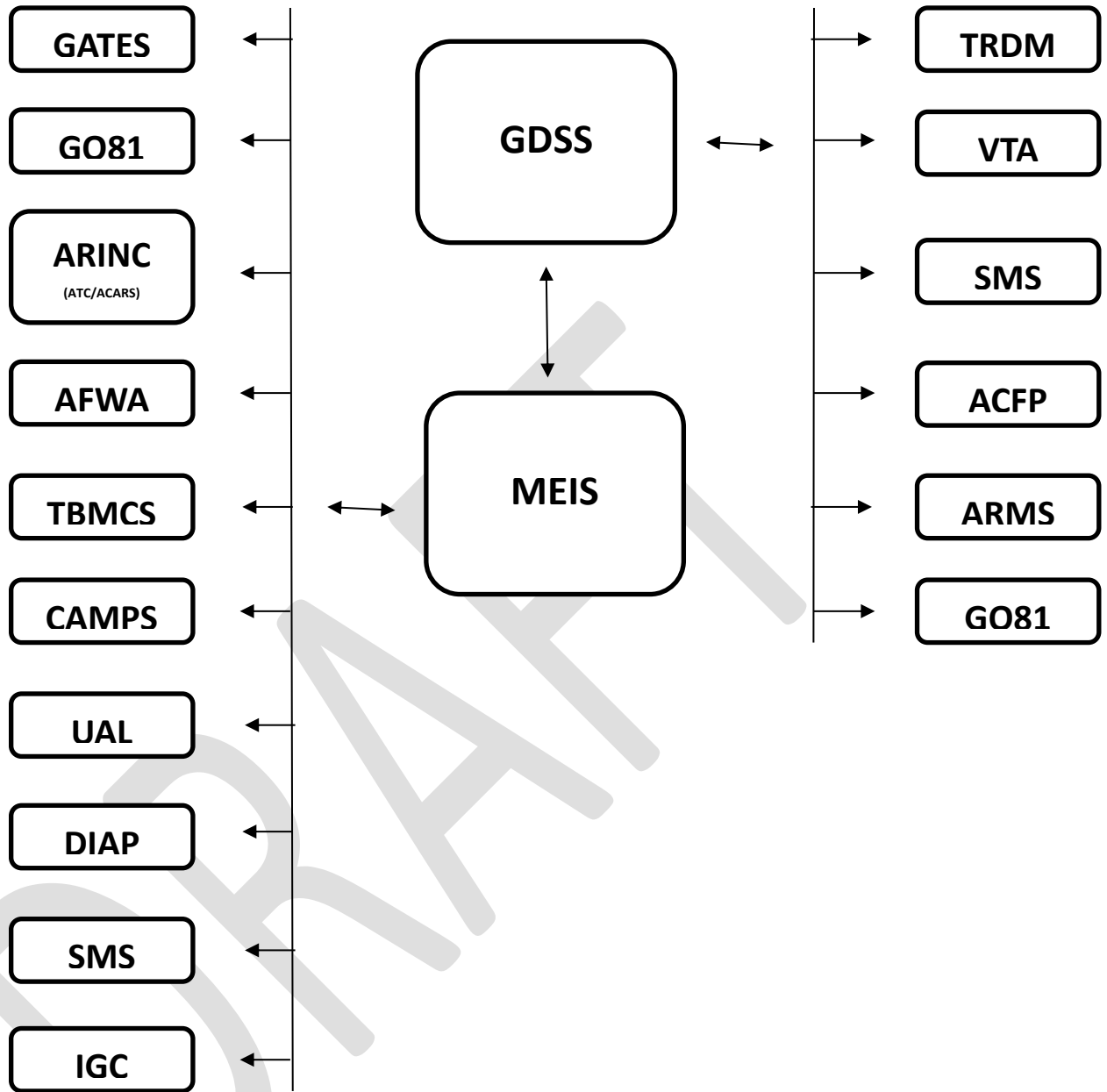


Figure 1-2: GDSS and System Relationships

1.4 Objectives

The objective of this Performance Work Statement (PWS) is to establish GDSS Application Support Services. The contractor shall collaborate closely with HQ AMC/A6IM to maintain each force package's integrity. The resulting heightened situational awareness will allow HQ AMC/A6IM leadership to take pro-active mitigation steps or eliminate obstacles to mission execution.

1.5 GDSS Stakeholder Team

1.5.1 The GDSS team consists of Government and contracted support working together to support the customer. Representing the customer is the Functional Manager (AMC/A3CS), contracting support is 763 SCONS working in concert with the Program Support Branch (AMC/A6IS), budget and other resources support comes from AMC/A6XR. The GDSS Program Management Office (PMO), under A6IM is the Office of Primary Responsibility for managing the system sustainment.

1.5.2 A6IS also manages the primary software systems support contract; Applications Infrastructure and Systems Support (AISS). AISS provides systems engineering, testing, training, technical and fielding support. The GDSS operational Systems Manager and software security support is provided by the 375th Airlift Wing. The Maine Air National Guard provides hardware logistics.

1.5.3 CROSS UTILIZATION OF RESOURCES: The Contracting Officer's Representative (COR) will not discourage any Contractor to take measures that may reduce overhead by way of sharing administrative resources within the company, however, the Government will not accept, as an excusable delay, that the Contractor's engineers, database administrators, or other technicians have been assigned to other contracts.

2. Scope

The tasks to be accomplished are in support of the HQ AMC/C2 System Branch (HQ AMC/A6I) GDSS PMO. The PMO manages the System of Record (GDSS). The term 'GDSS' includes several peripheral items: Interfaces and Information Services, a number of sub-applications, sub-systems, and projects that require support from the Contractor. Projects under the program may be added, transferred, or disbanded throughout the contract performance period. AMC/A6I programs utilize the Software Engineering Institute (SEI), Capability Maturity Model Integration for Acquisition (CMMI-ACQ) Level 3 as the model baseline in its efforts to improve overall program management of software releases and program support/integration.

2.1 Systems Sustainment

GDSS is now in a sustainment phase. Development is required but limited to Corrective, Adaptive, Enhancement, or Perfective Maintenance (IEEE Std 1219-1998):

- Corrective – The reactive modification of a software product performed after delivery to correct discovered problems. NOTE: The modification repairs the software product to satisfy requirements.
- Adaptive – The modification of a software product, performed after delivery, to keep a software product usable in a changed or changing environment. NOTE: Adaptive maintenance provides enhancements necessary to accommodate changes in the environment in which a software product must operate. These changes are those that must be made to keep pace with the changing environment. For example, the operating system might be upgraded and some changes may be made to accommodate the new operating system.
- Enhancement - Deletion and addition of functions to sustain warfighter capabilities, the adaptation to changes in data requirements and operation environments, the improvement of performance, usability, or any other quality attribute.
- Perfective - Modification of software after delivery to improve its performance or maintainability.
- AMC/A6IM uses the International Organization for Standardization (ISO) definition for "maintenance" for the same purpose: (paraphrased) "The maintenance process contains the activities and tasks of the maintainer. This process is activated when a system undergoes modifications to code and associated documentation due to an error, a deficiency, a problem, or the need for an improvement or adaptation. The objective is to modify an existing system while preserving its integrity."
- Contractor shall provide GDSS system releases in a non-service interrupted process.
- Contractor shall provide sustainment and integrated support for Mobility Enterprise Information Service (MEIS) 3.x/MGOP until otherwise directed by the GDSS PMO.

3. Requirements/Description of Services

The Contractor shall provide support in fielding and operational maintenance.

The Contractor shall provide the GDSS PMO with administrative support to meet financial and programmatic reporting needs and shall implement agile development activities.

The Contractor shall comply with the appropriate DOD, Services, USTRANSCOM, and AMC architectures, programs, policies, standards and guidelines (e.g., Strategic Technical Guidance [STG], Net-Centric Enterprise Services [NCES], and Defense Information Systems Network [DISN]).

GDSS Contractor responsibilities include: responsiveness, cost control, schedule management, a cooperative teaming environment, quality, resource management, and a commitment to customer satisfaction. Except for those items specifically stated as Government-furnished, the Contractor shall furnish everything needed to perform this contract. In the absence of specific contract requirements, the Contractor shall use the software development industry standards and industry best practices for providing the products and services required by the contract. The Contractor shall perform the following tasks:

- Task 1 – Enterprise IT Policy and Planning
- Task 2 – Integrated Solutions Management
- Task 3 – Market Research and Prototyping
- Task 4 - Custom Application Development
- Task 5 - Asset Management
- Task 6 - Security Engineering Certification and Accreditation
- Task 7 - Operations Support
- Task 8 – Hardware
- Task 9 - Optional Additional MAJOR RELEASE

3.1 Task 1 – Enterprise IT Policy and Planning.

In providing plans, reports and technical assistance, the Contractor shall accomplish the following:

3.1.1. Subtask 1 – Program Management. The Contractor shall provide the planning, direction, coordination, and control necessary for effective and efficient accomplishment of all requirements contained in this PWS. This effort shall be consistent with the PWS and Government-approved plans, schedules, and milestones. The Contractor's Project Manager shall coordinate work carried out under this PWS with the appropriate Contracting Officer's Representative (COR). The Contractor shall meet stated Government requirements and milestones and must advise the COR as soon as possible whenever requirements and milestones cannot be met. Actual or projected failure to meet PWS requirements and milestones shall be orally reported to the COR as soon as the information is available and also in the appropriate periodic reports, test reports, and review minutes. Contractor proposals for corrective action shall also be provided to and approved by the COR for all reported actual or projected failure.

3.1.2. Subtask 2 – Documents. The Contractor shall prepare, submit, and maintain the following documents:

Plans and Agreements

- Management Plan
- Quality Program Plan
- Technical & Management Work Plan
- Configuration Management Plan
- Software Development Plan

Contract Data Requirements List (CDRL)

(CDRL A001)
(CDRL A002)
(CDRL A003)
(CDRL A004)
(CDRL A005)

Reports and Documents

- Contract Performance Report (CPR) (CDRL B001)
- Task Schedule Progress Review (TPR) (CDRL B002)
- Integrated Master Schedule (CDRL B003)
- Equipment Inventory Records (EIR) (CDRL B004)
- Scientific & Technical Reports (CDRL B005)
- Software Test Report (STR)/Software Test Description (STD) (CDRL B006)
- Agenda/Minutes (CDRL B007)
- Test Readiness Review Report (CDRL B008)
- Contract Work Breakdown Structure (CWBS) (CDRL B009)

Procedures & Descriptions

- Test Procedures/Cases (CDRL C001)
- Interface Requirements Specification (CDRL C002)
- Interface Design Description (CDRL C003)
- Database Design Description (CDRL C004)
- Software Design Description (CDRL C005)
- Software Version Description (CDRL C006)
- Software User's Manuals (CDRL C007)
- System/Subsystem Design Description (CDRL C008)
- Computer Software End Items (CDRL C009)
- GDSS Installation & Operations Document (CDRL C010)
- What's New Document (CDRL C011)
- Requirements Specification Agreement (RSA) (CDRL C012)

Change Requests (CRs)

- Baseline Change Request (BCR) (CDRL D001)
- Software Problem Report (SPR) (CDRL D002)
- Document Change Request (DCR) (CDRL D003)

Other

- Engineering Change Proposal (CDRL E001)
- Request for Deviation (CDRL E002)
- Training Conduct Support Document/Training Lesson (CDRL E003)

The Engineering Change Proposal, Requests for Deviation, Document Change Requests, SPRs (Software Problem Request - changes required to correct errors or code that is not working or does not meet expected functionality), and BCRs (Baseline Change Requests - changes requested by the COR to upgrade or change a function in the software) will often require input from the Contractor. Change Requests (CRs) shall be written in a clear concise manner. See Attachment 3 for examples of SPRs and BCRs.

3.1.3 Subtask 3 – Support and Attend Meetings and Conferences. This subtask addresses CDRLs A003, B001, B002, B003, B005, and B007. The Contractor shall attend the following meetings:

3.1.3.1 Contract and Program Status Review. The Contractor shall host this monthly meeting at an agreed upon location. The contractor shall prepare an agenda and provide written minutes (CDRL B007). The purpose of this meeting is to review and update the Contractor's Technical & Management Work Plan (CDRL

A003), brief the progress of each assigned task (CDRL B001), address schedule tracking concerns/impacts to the master schedule (CDRL B003), review financial status, and solicit input from the PMO to obtain concurrence of work performed by the Contractor.

3.1.3.2 Provide Contract Performance Report. The presentation of the CPR with slides or other presentation material provided to the Government meets the requirement for this report (CDRL B001).

3.1.3.3 Task Schedule Progress Review (TPR, bi-weekly) (CDRL B002)

3.1.3.4 Other meetings routinely attended by the Contractor:

- Program Management Review (PMR, monthly)
- CIO Program Review Process Preparation (CPRP) (Monthly)
- Support Ad Hoc Teams (average 1 per week)
- Security Working Group (average 1 per week)
- Performance Teams (average 1 per week)
- Accreditation Support (as required for releases, annual reviews, and re-accreditation)
- Document update meetings (as architecture changes or software releases dictate)
- Technical Working Group (TWG) Support (historically weekly)
- GDSS Weekly Updates (GWU)
- Host backlog reviews, sprint demonstrations, application design, collaborative testing (COLT), and other sustainment meetings as required by the GDSS PMO.

3.1.3.5 The Contractor shall generate presentation materials if required to aid in the discussion of meeting topics and shall support conferences, meetings, demonstrations, and Technical Interchange Meetings/Reviews (CDRL B005). For meetings that the Contractor is required to host, they shall provide agendas, meeting minutes, and track action items associated with the aforementioned meetings/reviews (CDRL B007).

3.1.4 Subtask 4 – Task Schedule Progress Review (TPR). This subtask addresses CDRLs A001, A003, and B003. The Contractor shall provide visibility/monitoring of task progress by accomplishing the following:

3.1.4.1 Maintain and annotate a project schedule of all Contractor activities associated with the efforts described in tasks 1 through 5 utilizing the tools identified by the Government. The format of the project schedule shall be as agreed with the COR to assure readability (CDRL B003).

3.1.4.2 Populate each schedule with sufficient task activities to ensure visibility of management and tracking for each milestone (CDRL A003).

3.1.4.3 Identify, within the schedule, the resources required to accomplish all task activities. Contractor may use generic resource identification (CDRL A001).

3.1.4.4 Collaborate with the PMO to determine and annotate appropriate milestones needed to

ensure/monitor progress (CDRL A003).

3.1.4.5 Baseline all schedules with concurrence of the COR (CDRL B003).

3.1.4.6 Update schedule progress on a weekly basis using Government-provided tools (CDRL B003).

3.1.4.7 Provide schedule status, risks, issues and progress (CDRL A001).

3.2 TASK 2 - Integrated Solutions Management

3.2.1 Subtask 1 – System Integration. This subtask addresses B005, B006, B007, C001 through C011, and E003. The Contractor shall support full system integration by ensuring that the software does not adversely affect the intended operational system, and by accomplishing the following tasks:

3.2.1.1 Prepare and deliver the end items of the intended operational system (CDRL C001, C009, and C010).

3.2.1.2 Ensure and demonstrate that the software is integrated into the intended system configuration.

3.2.1.3 Provide software application training for key technical personnel, functional help desk personnel, trainers, testers, and others if designated by the COR for each release. This has been referred to as "train the trainer", the objective being that any software changes that affect the operating procedures shall be taught to the key personnel that support the program (CDRL E003).

3.2.1.3.1 Training Conduct Support Document, DI-SESS-81523B, with the following deletions: paragraphs 2.2.2.ae. With the COR's approval, the Contractor may deviate (add and delete) from the Training Conduct Support Document/Training Lesson (TCSD/TL) Data Item Description (DID) content requirements in order to further tailor the TCSD/TL to the Missions Systems training culture and the Contractor's training strategy. However, the Contractor shall explain in an executive summary or an addendum to the TCSD/TL its rationale for adding or deleting a specific DID requirement. Nevertheless, the COR retains the right to require any part of or all of the Data Item Instructions to be adhered to by the Contractor. Each version release and some patches may require a TL. Outline TL due 30 days prior to each planned version release (CDRL E003).

3.2.1.4 Final TL due 30 days prior to version fielding (CDRL E003).

3.2.1.5 Provide GDSS technical remote and hands-on support to the teams installing and fielding the delivered system.

3.2.1.6 Prepare and deliver software releases and test results, including all required components and documentation (CDRLs B005, B006, B007, and C001 through C011).

3.2.2 Subtask 2 – Additional Integration Efforts. This task area includes management and technical support for research, analysis recommendation and documentation of integration issues and approaches. The issues and approaches considered under this area evolve from a variety of sources such as external audits, technical reports, Federal standards, operational policies and doctrines, technical guidelines and best practices. The Contractor shall perform the following activities for services required under this task area:

3.2.2.1 Examine functional and technical requirements and/or issues to provide effective solutions for integration efforts that include:

- Review technical solution(s) to operate within the AMC designated C2 and In-Transit Visibility (ITV) designed architecture and interoperate with other C2 and ITV systems
- Compliance with Legal and Regulatory Guidance
- Net-Centricity—Integrate data and business rules requirements with other DOD, Federal,

USTRANSCOM or AMC data integration efforts

- Architectures – Provide technical drawings consisting of recommended solutions that may be used to develop AMC architectural products
- Security Compliance
- Benchmarking/Baselining
- Performance
- If directed, develop prototypes as proof of concepts

3.2.2.2 Develop documentation resulting from studies, analyses, assessments, and engineering designs. Documentation may include subject matter originated by the Contractor as well as Government-provided topics. Document enhancements to existing system architecture to take advantage of the infrastructure environment proposed. Data items to be delivered under this optional subtask shall be identified in each contract.

3.3 TASK 3 – Market Research and Prototyping

3.3.1 The Contractor shall evaluate COTS and other solutions to support GDSS applications, and other special equipment requirements. The Contractor shall actively evaluate the COTS and other solutions, such as features and functionalities, for opportunities to correct inefficiencies, errors, and recommend solutions. This includes established efforts to migrate the current software to an updated platform chosen by the COR. The Contractor shall assist the Government by testing Government chosen products and making recommendations (CDRL B005).

3.4 TASK 4 – Custom Application Development

3.4.1 USTRANSCOM has directed GDSS to migrate to a commercial Cloud environment and to utilize a DevOps paradigm. For Cloud Integration, the contractor will utilize USTRANSCOMs DevOps model (tools, methods and processes). Any deviation from DevOps model must be approved by the USTRANSCOM TCJ6 Enterprise Change Control Board (CCB). The developer is required to provide all software assets required to build, deploy, test, operationalize and run an application.

3.4.2 Primary Systems under this task: The primary systems are engineered and developed by the Contractor. The physical environments for the systems are engineered and maintained under a separate support contract. These include the operational environments housing the active applications the customers are using around the world. The Contractor shall provide written (CDRL B005) or verbal installation instructions and assistance when technical guidance is required. If verbal instructions are provided, those instructions shall be included in the written format and schedule will be negotiated at time of request. The Contractor shall provide assistance when technical guidance is required for the following as required. GDSS is a system of several sub-applications centered on different types of users. This contract focuses on GDSS and its many sub-applications. The Contractor shall develop solutions to meet Government-directed changes and upgrades as required. The Contractor shall adhere to industry best practices during development to include security engineering.

3.4.3 GDSS Applications – provide standalone applications operating on multiple operating systems, e.g. iOS, Android, Windows, etc. Applications will be used in multiple environments, for example, Electronic Flight Bag (EFB). These applications shall be based on user community requirements and shall be created and delivered within the context of the overall GDSS program sustainment schedule.

NOTE: The interdependencies of the following systems and subsystems shall be tracked by the Contractor to ensure the fielding of individual subsystems maintains uninterrupted service to the customer.

3.4.3.1 Mobility Communications Services (MCS) – SOA component used to enable communication between

GDSS and MEIS 4.x.

3.4.3.2 Aviation Operational Risk Management (AvORM) – Sustainment is unique and limited to Corrective, Adaptive, Enhancement, or Perfective Maintenance (IEEE Std 1219-1998).

3.4.3.3 Exercise Management Console (EMC) – Used to support exercise execution in the TACC.

3.4.3.4 GDSS Training Applications – Applications can be loaded onto a system and utilized to train with real-world representative scenarios.

3.4.3.5 Security patches, Time Compliant Network Orders (TCNOs), and Group Policy Objects (GPOs).

3.4.3.6 Other – Other projects are expected to emerge

3.4.3.7 GDSS Testing Suite

3.4.3.8 GDSS Prototype Suites

3.4.3.9 GDSS Training Suites

3.4.3.10 GDSS Exercise Suites

3.4.3.11 Enterprise Services Management (ESM) – Contractor shall work with AISS contract personnel to assist with script development for system health monitoring purposes, as requested by the PMO.

3.4.3.12 Provide support to utilize Mobility Automated Cross Domain (MAC-D) solution as required.

3.4.3.13 USTRANSCOM Situational Awareness (SA) Common Operational Picture (COP) – This provides proactive ability to identify whether a system is accessible to and usable by the user community

3.4.4 Subtask 1 – Configuration Management (CM). The Contractor shall provide a software configuration management plan/process that incorporates the following:

3.4.4.1 Using MIL HDBK 61A, ISO/IEC 12207:2008, and EIA 649-B guidance, the Contractor shall institute and maintain a configuration management process to ensure engineering and administrative disciplines (which include configuration identification, configuration control, status accounting, and auditing) are implemented for all development and GDSS Functional Help Desk activities. The Contractor shall identify the configuration of all work products (to mean multiple baselines as well as other supporting work products); systematically controls changes, and maintain the integrity and traceability of all work products throughout their lifecycle. The Contractor shall ensure configuration is identified, reliable, traceable, and repeatable, and that all relationships among work products, versions of work products, as well as auditing and reporting on the changes that are made are implemented throughout the development process. Authority: DI-SESS-81875. Finalize with the COR NLT 20 business days after award.

3.4.4.2 In addition, the Contractor shall accomplish the following:

3.4.4.2.1 Establish and employ internal configuration management of processes and procedures for all development work products.

3.4.4.2.2 Identify the configuration items (including COTS software), components, and related work products, to include baseline documentation, and place these items under configuration control.

3.4.4.2.3 Establish and maintain a configuration management and change control system for controlling configuration items, components, and work products.

3.4.4.2.4 Establish version control to ensure integrity and tracking of all work products.

3.4.4.2.5 Identify, track, and control change requests (including those changes intended to resolve identified problems) for the configuration items.

3.4.4.2.6 Establish configuration control of all supporting documentation, changes to the documentation, and version control of all documentation supporting work products, and ensure product documentation reflects all changes to a work product.

3.4.4.2.7 Provide backup controls to ensure work products are not lost or damaged due to resource, equipment, or power failures.

3.4.4.2.8 Establish and employ product CM processes and procedures to ensure the integrity of all delivered baselines and work products.

3.4.4.2.9 Establish and maintain records describing configuration items.

3.4.4.2.10 Ensure internal controls are in place supporting all baselines and work products.

3.4.4.2.11 Ensure configuration audits are available supporting the integrity of the configuration.

3.4.4.2.12 Ensure the internal configuration status accounting system records the tracking of baselines and work products and their modification history throughout the life cycle.

3.4.4.2.13 Configuration controls shall ascertain the content of any delivery, baseline or work product is accurate and complete, and unaltered upon delivery. In the case of code delivery, a Government issued digital signature shall be affixed to code before delivery, to ensure the code was not altered.

3.4.4.2.14 Record and present to the COR, the results of the configuration audit, to include action taken by the Contractor to correct deficiencies noted during the audit. The Contractor shall correct all deficiencies noted during the audit prior to presenting the deliverable for Government acceptance.

3.4.4.2.15 Coordinate closely with PMO or the designated Configuration Manager to ensure continuity of configuration management processes and practices are maintained and controlled.

3.4.4.2.16 Ensure development CM processes and procedures compliment the Government's Configuration Management Plan (CMP).

3.4.4.2.17 Provide traceability and visibility to the PMO for all CRs throughout the system lifecycle via a requirement traceability tracking tool. Additionally, access to user stories, backlog lists, and other artifacts shall be made available to the GDSS PMO upon request.

3.4.4.2.18 CM of software shall include a comprehensive method of recording all COTS software purchase and warranty dates, support and warranty expiration dates, and a plan to provide adequate lead time to extend or replace warranties or support as needed.

3.4.4.2.19 The Contractor should understand with the migration to a commercial Cloud and implementation of a DevOps paradigm there may be necessary adaptive changes to configuration management processes and the Contractor shall agree to implement those processes as necessary.

3.4.5 Subtask 2 – Quality Control. Provide a Quality Control Program explained in a Quality Program Plan (A002) that incorporates the following:

3.4.5.1 The Contractor shall provide a single point of contact (POC), and alternate POC, for Government to Contractor, day to day business and quality control. This does not preclude routine contact between the COR and Contractor administration and technicians as required, but all official communications relating to contractual effort, cost, schedule, performance, and changes in resources shall include that POC. Customarily this will be the local site or business manager of the company, and/or the company representative to the Contracting Officer (CO).

3.4.5.1.1 The Contractor POC shall be the first line of communication in settling any minor issues not requiring intervention of the CO.

3.4.5.2 The Contractor shall establish and maintain a Quality Control Program in accordance with ISO IEC 26514:2008 and SEI CMMI Level 3-Defined requirements or equivalent processes approved in writing by the COR. In establishing and maintaining a Quality Control Program, the Contractor shall plan, develop, and implement procedures and practices to ensure that all requirements of the contract are complied with fully. The COR shall audit all processes and products as outlined in the Quality Control Program Plan. The Quality Control Program Plan shall also include a non-compliance reporting and tracking process.

3.4.5.3 The Contractor shall support Government reviews and audits of all services and support provided under this contract. The Government reserves the right to authorize an independent verification and validation of the Contractors' procedures, methods, data, equipment, and other services provided at any time during the performance of this contract. At the COR's discretion, registered ANSI/ISO/ANSQ Q9000 series suppliers may not be subjected to audit/assessment by the Government if they provide the COR with a copy of their registration certification issued by an approved ISO registrar.

3.4.6 Subtask 3 – Interoperability and Architecture Support. This subtask addresses CDRLs B005, C008, and E001. The Contractor shall provide interoperability and architecture support by accomplishing the following tasks:

3.4.6.1 Ensure that the technical designs and system elements comply with the Defense Information Technology Standard Registry (DISR) (CDRLs B005, C008, and E001).

3.4.6.2 Design technical solutions to operate within the GDSS framework, and interoperate with other systems.

3.4.6.3 Ensure technical design and solutions are compatible with DOD infrastructure, e.g., Standard Desktop Configuration (SDC), operational environment, and Group Policy Objects (GPOs).

3.4.6.4 Participate in developing and validating Department of Defense Architecture Framework (DoDAF) products. The Contractor shall use AMC Architecture Tool (AMCAT) AMC's Consolidated Architecture Tool Suite (CATS) for the source of all DoDAF compliant architectures

3.4.6.5 Participate in supporting Air Force, Joint, and Federal agencies certifications.

3.4.6.6 Develop prototypes as proof of concepts.

3.4.7 Subtask 4 – Software Release Process. This subtask includes CDRL C009.

3.4.7.1 The Contractor shall provide the support necessary to maintain the GDSS software via the Government's sustainment and approval processes. The GDSS program utilizes multiple methods, to include traditional Waterfall, Agile or a combination of the two for software sustainment. Examples of these methods, coupled with Government approval processes are depicted in Figures 3-1 and 3-2. Future releases, (i.e. converting functionality into individual applications) benefit from utilizing "Agile" principles, such as Sprint Planning, Sprints, Scrums, and Incremental deliveries. The Contractor shall provide recommendations on the optimum development process and the Government shall determine the final method and processes utilized for each release. GDSS produces a Requirements Specification Agreement (RSA) through its configuration control boards

and Joint Functional Management Board (FMB) creation of a prioritized requirements listing. The details for the individual requirements are maintained in a database.

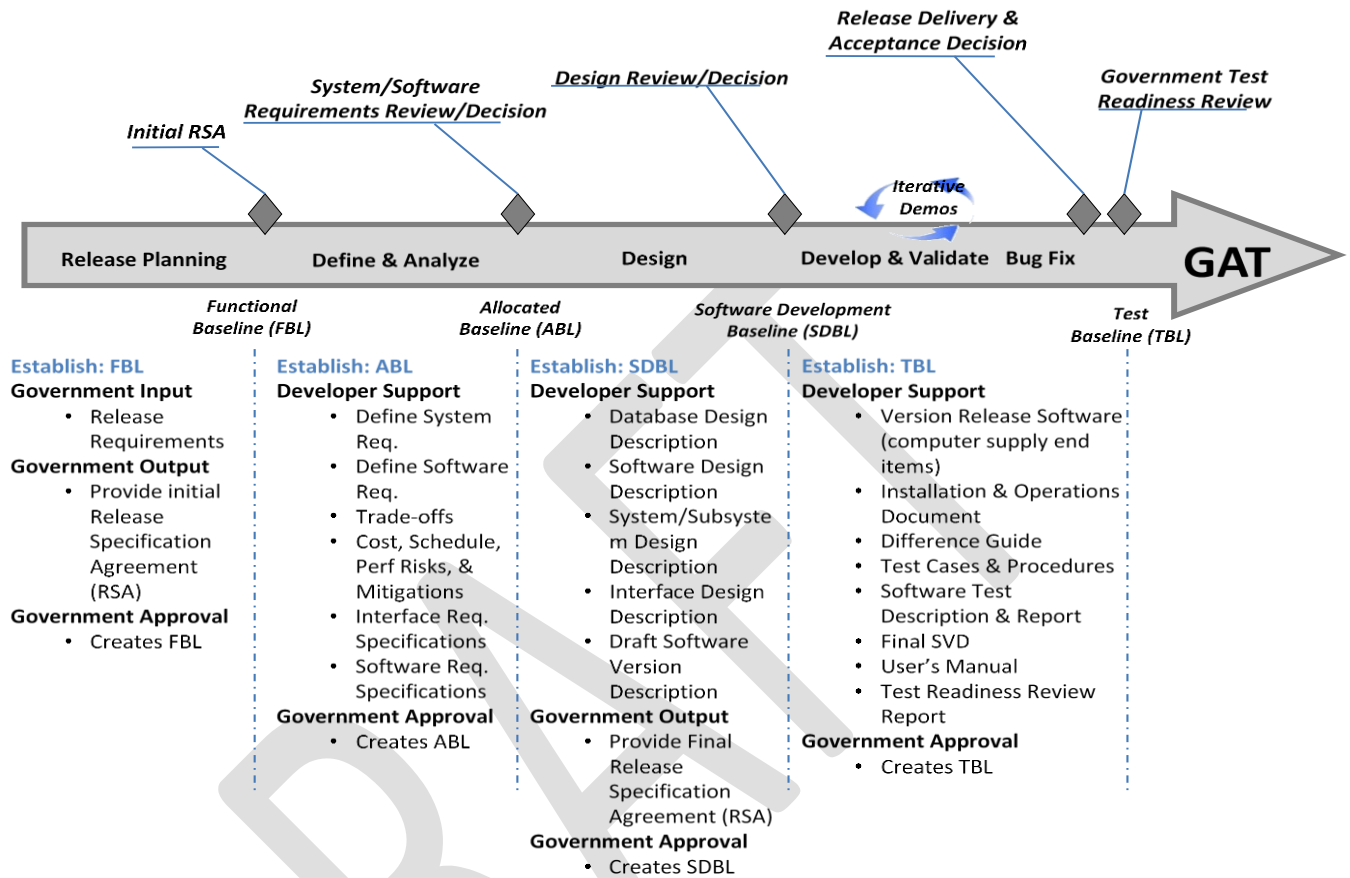


Figure 3-1: Waterfall

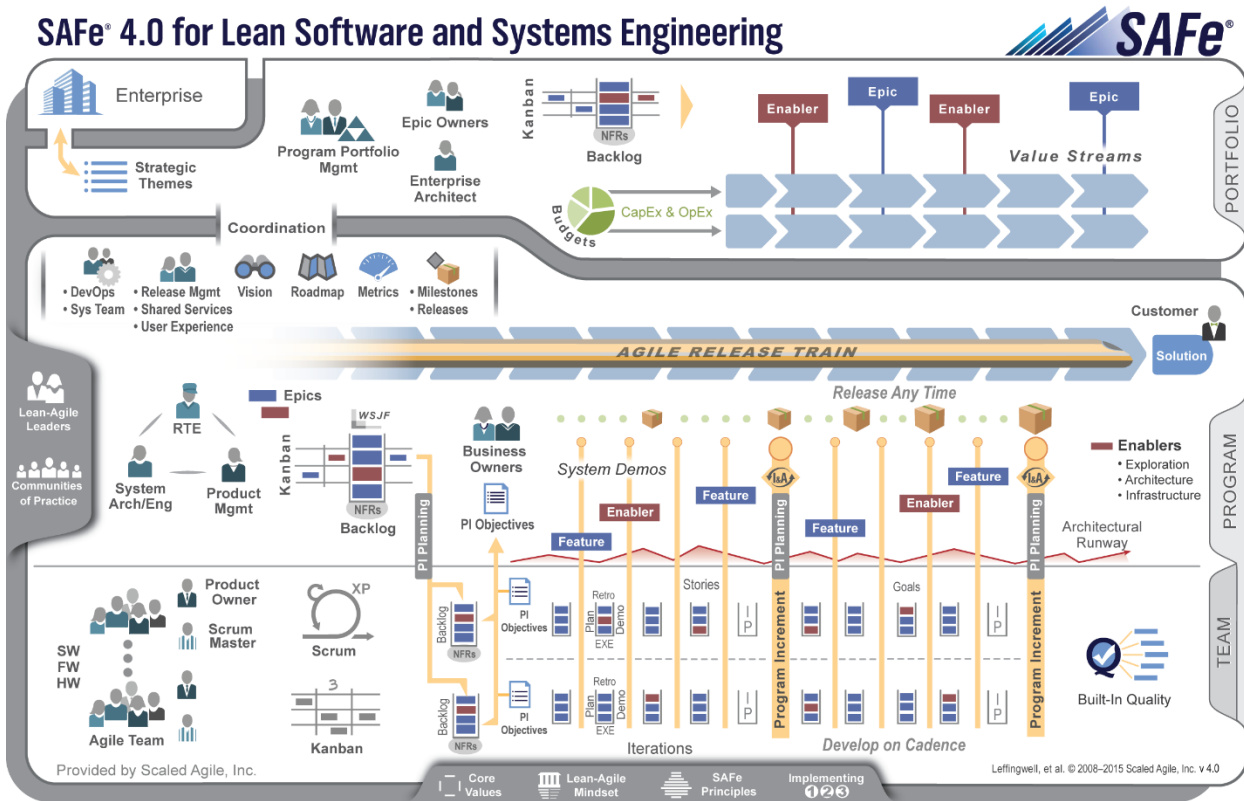


Figure 3-2: Agile

3.4.7.2 MAJOR RELEASE FREQUENCY. The Contractor shall deliver two major releases (Core GDSS) per each period of performance supporting GDSS (CDRL C009). Major releases include software modifications for COTS updates, security changes, and multiple functional updates as required due to changes in business rules, interface changes, or technical configuration changes. A major release is considered a roll-up of requirements (historically 70-130 requirements) into a single package. The number of requirements will be determined and prioritized by the Government. If agile development is utilized, multiple incremental deliveries will be rolled up to produce a single major release. Delivery dates and schedules are developed on a continuing basis based on requirements to develop, resources available to field and maintain them, and the interdependencies with other systems and their schedules. When external events create delays, the Contractor shall demonstrate the capacity to deliver these two major deliveries and may be required to deliver code that will have to be 'shelved' until fielding is possible. This will include the application transition support for GDSS.

3.4.7.3 MINOR RELEASE FREQUENCY. The Contractor shall deliver up to 8 minor releases (AvORM, EMC, special patch packages) per each period of performance (CDRL C009). The scope of a Minor Release is such that would not constitute a Major Release; however, would exceed that of a small sustainment software delivery. Although not always the case, the scope of a Minor Release might require the contractor to manage resources and schedules in order to minimize the impact to other efforts that includes the current Major Release being worked.

3.4.7.4 Corrections/Hot Fixes/Warm Fixes/Patches. The Contractor shall deliver up to 120 small sustainment software deliveries to include patches, hot fixes, small scale changes to GDSS or any of the other systems/subsystems. While not always the case, small sustainment software deliveries are generally short in duration, small in effort, utilizing few engineering resources, focused on a single issue or lower in complexity, often unplanned, and have little or no impact to the major release schedule. Credit for a small sustainment

software delivery release is granted when the Contractor responds to operational issues and provides a solution.

3.4.8 Subtask 5 – Analyze. This subtask addresses CDRLs B005, C006, C012, D001, D002, D003, and E001. The Contractor shall provide analysis support by accomplishing the following tasks:

3.4.8.1 Analyze effort required to produce system ready software. This analysis addresses the efforts in the process leading to the 2nd milestone; System Software Requirements Review. Contractor shall analyze individual requirements and the collective content of a planned release and provide the COR with an estimate on a rough order of magnitude (ROM) of the effort required for development (B005, E001).

3.4.8.2 A ROM (B005) may be requested by the COR for any one or more CRs for the purpose of sequencing them into releases or other reasons. ROMs shall include total hours per CR. When a ROM is requested for a release the Contractor shall provide the total hours, proposed delivery schedule and cost for the release. These ROMs are generally expected to take 1-3 weeks to complete for a standard major release. Additional time will be coordinated if refining/defining of requirements are needed. An estimated 30 ROMs per year may be expected.

3.4.8.2.1 When a request for a ROM is made, the Contractor shall first provide an estimate of when the ROM will be complete. The ROM completion date shall be provided before the closing of the following working day.

3.4.8.3 When requested, propose refinements and analysis to use cases, CRs (BCRs and SPRs) (CDRLs D001, D002, D003), user stories, and backlog items in accordance with business practices, processes, procedures, systems, and performance measures. The Contractor shall be responsible for assuring they are completely understood by the engineer addressing them. See Attachment 3 for standards for CRs.

NOTE: For the purpose of this PWS, 'CRs' and 'Requirements' are similar and used interchangeably in discussion. While a CR may be called a requirement, they emerge from several sources, and must be refined with all the aspects of a complete requirement before development is carried out.

3.4.8.4 Conduct version planning sessions to refine/define software requirements specifications (CDRLs B005, C006, and C012).

3.4.8.5 As a result of meetings or analysis, propose changes to business practices, processes, procedures, systems, and performance measures (CDRL B005).

3.4.8.6 Analyze and, , provide recommended changes to version requirements documents/lists (CDRL C006, C012).

3.4.8.7 Analyze and, , provide recommended changes to the requirements list test pass/fail criteria (CDRL B005).

3.4.9 Subtask 6 – Design. This subtask addresses CDRLs C002, C003, C004, C005, C006, and C008. The Contractor shall design software to meet requirements by completing the following tasks:

3.4.9.1 The Contractor shall meet the plans, specifications, and descriptions accepted by the COR under Task 1. The Contractor shall design and document software architecture, including incorporating business rules. Additionally, the Contractor shall prepare design products to support technical review and approval of the next steps the Contractor will take in the development phase (CDRLs C002, C003, C004, C005, C006, and C008).

3.4.9.2 Conduct design reviews.

3.4.9.3 Provide sustainment and configuration management of the system-centric Physical Data Model (PDM)

and Data Dictionary.

3.4.9.4 Use Government reference data source, currently provided by USTRANSCOM Reference Data Management (TRDM) System, as the authoritative source of system reference data.

3.4.9.5 Participate in the Architecture Data Integration Group (ADIG) to assist the Government with the sustainment and configuration management of the Government-provided enterprise-level Logical Data Model (LDM) and the Data Dictionary.

3.4.9.6 Assist the Government in the sustainment and configuration management of the system-centric LDM and mapping of the PDM to the Government-provided Enterprise LDM.

3.4.9.7 Submit proposed Service Definition schemas to the COR for approval prior to establishing a system/service or interface.

3.4.9.8 Participate in working group assisting the Government in the sustainment and configuration management of the Government-provided enterprise-level and system centric Interface Design Documents and Services Definition Framework.

3.4.9.9 Assist the Government in the identification, creation, update and/or deletion, and documentation of reference data, e.g., port names.

3.4.9.10 Assist the Government in selecting the appropriate software development process, e.g., waterfall, spiral, agile.

3.4.10 Subtask 7 – Establish and Maintain Development Environment (Optional)

NOTE: Development shall take place in a controlled Contractor environment or Government facilities, and shall not be accomplished outside of these environments.

3.4.10.1 Use GFE to establish and maintain a development environment reflecting the most current operational configuration.

3.4.11 Subtask 8 – Developer-to-Developer Mobility Network (MOBNET) (Optional)

NOTE: Development shall take place in a controlled Contractor environment or Government facilities, and shall not be accomplished outside of these environments.

3.4.11.1 Use GFE to establish and maintain an environment that can be accessed by external users to develop software or other applications in an integrated manner with other C2 applications/systems.

3.4.12 Subtask 9 – Develop. This subtask addresses CDRLs B005, C001, C009, C010, and C011.

3.4.12.1 USTRANSCOM has directed GDSS to migrate to a commercial Cloud environment and to utilize a DevOps paradigm. For Cloud Integration, the contractor will utilize USTRANSCOMs DevOps model (tools, methods and processes) as directed, if needed. Any deviation from DevOps model must be approved by the USTRANSCOM TCJ6 Enterprise Change Control Board (CCB). The developer is required to provide all software assets required to build, deploy, test, operationalize and run an application that are not supplied by the government.

3.4.12.2 The Contractor shall develop software using an agile development method to sustain the GDSS capabilities as noted in paragraph 2.2. The scope/size of each release is based upon the Government requirements process that prioritizes the requirements before the Contractor estimates how many requirements can be included in the release based upon constraints such as time and funding. The COR then formalizes

what requirements are officially included in the release. It should be understood that all requirements are not equal in level of effort required to implement and cost to implement.

NOTE: Development shall take place in a controlled Contractor environment or Government facilities, and shall not be accomplished outside of these environments.

3.4.12.2 The Contractor shall maintain the development environment to the most current operational configuration.

3.4.12.3 Validate the intended release environment configuration prior to commencing development of a software release.

3.4.12.4 Coordinate immediately with the COR when deviations to the intended environment configurations are necessary to support development and delivery of the software release.

3.4.12.5 The Contractor shall develop, test, document, and deliver software solutions, including implementation of business rules such that it performs satisfactorily on Government-provided equipment (CDRLs C001, C009, C010, and C011).

3.4.12.6 The Contractor shall ensure that developed software does not interfere with currently fielded hardware or Government-accepted software.

3.4.12.7 The Contractor shall conduct unit code and database reviews to ensure the system, software, and database meets the approved technical design, specifications, and descriptions and is ready for developer testing. The Contractor shall ensure the system, software, and database includes implementation of business rules and industry best practices such that it performs satisfactorily on Government provided equipment, and interoperates and does not interfere with currently fielded hardware or Government accepted software.

3.4.12.8 The Contractor shall ensure a schedule is maintained to encompass all long lead items approved for development and associates each long lead item to a target release schedule. Manage development of each long lead item to ensure each item is ready to incorporate into its intended release.

3.4.12.9 The Contractor shall confirm vendor software patch compatibility with existing GDSS code.

3.4.12.10 The Contractor shall analyze and upgrade the database management system as required.

3.4.12.11 Opportune Fixes

3.4.12.11.1 The Contractor shall identify errors or inefficiencies in the code being worked for either changes or fixes. The Contractor shall make opportune fixes under the following guidelines:

3.4.12.11.2 The Contractor shall record errors identified in the code as they are discovered. Engineers shall not open code with the intent to seek opportune fixes as part of development of a scheduled release.

3.4.12.11.3 The Contractor shall proceed with any fix with no further coordination if the Time Factor and either of the Test Factors are applicable.

3.4.12.11.4 Time Factor: The fix to the error is minor and can be accomplished without any impact to delivery schedule.

3.4.12.11.5 Test Factor 1: The fix will not need to be tested in Government Test and Evaluation (GT&E) because it is a simple error or change that cannot have any impact on system operation. An example of this is to remove the '2' from GDSS2, in a field or graphic that has zero interaction with other fields or computations.

3.4.12.11.6 Test Factor 2: The fix will not add to the expected duration of GT&E.

3.4.12.11.7 If any fix will push the code delivery date by only one working day and GT&E testing will not need more than one additional day, the Contractor shall proceed with the fix. In this case the Contractor shall inform the PMO before the end of the following working day after the discovery.

3.4.12.11.8 If any fix will drive the code delivery date by more than one working day or GT&E testing of that fix will require more than one additional day, the Contractor shall coordinate with the PMO and provide an expected impact on schedule or testing. The decision to proceed in this case shall be at the discretion of the Program Manager (PM).

3.4.12.11.9 If any accumulation of minor fixes result in delays as described in (the previous paragraph) above, the Contractor shall notify the PMO and provide estimates; any further opportune fixes that will impact the schedule shall cease until approval is granted by the PM.

Note: The Contractor shall advise the PMO as soon as practical of any changes made so that GT&E can be prepared for additional items to be tested.

3.4.12.11.10 The GDSS PMO may identify specific items to be fixed or enhanced as opportunity arises. During normal duty hours the GDSS PMO shall respond with Government approval or disapproval within an hour of any request for opportune fixes (when required).

3.4.12.12 Innovations

3.4.12.12.1 The Contractor shall provide a short summary (B005) describing opportunities for incorporating innovations into GDSS every six months. Include with each summary a ROM, schedule, and impact to existing work cost and schedule. Innovations for the purpose of this paragraph are similar to the 'opportune fixes' noted in the previous paragraph, but larger in scope. The Contractor shall propose innovations that improve performance, functionality, or maintenance. If the innovation is approved by the COR, the Contractor shall submit a technical proposal (CDRL B005/E001) identifying the tasks to be performed, in process reviews to be conducted, testing to be accomplished, event schedule, acceptance criteria, and Service Summary requirements. These proposals shall be limited to major changes or several smaller related changes/updates. The innovations may apply to software or hardware or a combination.

3.4.13 Subtask 10 – Emerging Technology Integration

3.4.13.1 The Contractor shall integrate emerging technology into the software/firmware/hardware solutions supporting GDSS.

3.4.14 Subtask 11 – Test. This subtask addresses CDRLs B006, B008, and C001. The Contractor shall conduct testing and complete the following tasks:

3.4.14.1 Produce and maintain test cases and software test descriptions (CDRL C001).

3.4.14.2 Perform testing (e.g. unit, integration, system, regression, security, performance, collaborative testing (COLT)) to verify that the software meets test pass/fail criteria for each requirement contained in the RSA, backlog or sprint review (CDRL B008). As part of the cloud migration effort and transition to a DevOps strategy, the contractor shall utilizing a government approved automated software testing tool to accomplish testing.

3.4.14.3 Verify that the software does not interfere with currently fielded hardware or Government accepted software.

3.4.14.4 Conduct and participate with the COR on integrated testing, to include regression testing, to ensure the developed capability is suitable for delivery to the COR as the test baseline (as defined in the Defense

Acquisition Guidebook).

3.4.14.5 Participate and document with the COR to complete any DOD, Joint, Air Force or other governing body certification or accreditation testing for all security classification domains.

3.4.14.6 Contractor shall host collaborative testing (Government contracted testing of pre-release software). A Memorandum of Agreement will be established between the Contractor, the COR, and the System Support Contractor (currently known as 'AISS'), within 60 days of contract award.

3.4.14.7 Provide to the COR all testing artifacts (e.g. test results, Software Test Descriptions, Test Readiness Review Report) required to complete all Government acceptance testing (CDRL B006).

3.4.15 Subtask 12 – Provide data flow/topology diagram. For each major or minor release this document must be provided 45 days prior to delivery. These data flow/topology diagrams shall be provided for corrections/fixes/patches as requested by the GDSS PMO.

3.4.16 Subtask 13 – Create the "What's New Document." See sample document of Attachment 1. This subtask addresses CDRL C011. The Contractor shall provide a "What's New Document" describing the changes made for the applicable release. This document shall be written in language understandable to the functional community.

3.4.17 Subtask 14 – Deliver. This subtask addresses CDRLs C007, C009 and C010.

3.4.17.1 Deliverable is disk copies of code developed, to include source code and executables and all necessary tools (CDRL C009). The Contractor shall include with each version release and patch, an installation plan, a programmer's reference guide providing text description of the Application Programming Interface (API) data structure and algorithms, and the Software User's Manual (SUM), which shall include the GDSS User's Manual (GUM) (CDRL C007). It is important for the code documents/reference guides to be thorough, but not so verbose that it becomes difficult to maintain them.

3.4.17.2 The Contractor shall prepare two copies on CD/DVD (or electronically), the executable software to be transitioned to the support site, including any batch files, command files, data files, environment group policy, or other software files needed to install and operate the software on the target computer(s).

3.4.17.3 Each CD/DVD shall contain the contract number, order number (if applicable), the title "GDSS", version release number (patch number, if applicable), date the CD was populated, and the number of CDs (e.g., 1 of 6, 2 of 6) for each copy of the CD. Each CD shall contain, either on the CD or in a Read Me file, the following statement: "The Government has unlimited rights to use, modify, reproduce, perform, display, release, or disclose the software delivered herein, in whole or in part, in any manner, and for any purpose whatsoever, and to have or authorize others to do so."

3.4.17.4 Format – Executable and operational within GDSS operating system.

3.4.17.5 Computer compatibility requirement – Meets GDSS system approved baseline configuration for acceptance testing.

3.4.17.6 The GDSS Installation Plan (CDRL C010) shall include the events/installation schedule (with site POC), site preparation procedures, installation procedures (including corrective actions if a problem arises), coordination plan (detailing how functional and site communications will be done and what outages are required), installation checklist, and notification plan (advertising that the installation is happening, who the POCs are, explaining the sequencing as to when, where, and how installs will be performed).

3.4.17.7 The Contractor shall understand with the migration to a commercial Cloud environment and the implementation of DevOps processes the details of the delivery process may need to be tailored for such

technologies and the Contractor shall be able adapt to these changes.

3.5 TASK 5 – Asset Management. The Government will provide property for the Contractor to use in the performance of the contract. The Contractor shall account for and maintain all the Government Furnished property (GFP), materials, and equipment in accordance with the Government Property clause included in the contract. GFP includes Government Furnished Equipment (GFE), and software provided by the Government. Meeting this task requires the following per DOD guidance:

3.5.1 Subtask 1 – Government Furnished Equipment (GFE). The Government will upon contract award provide workspace office equipment necessary for performance of this GDSS Application Support contract for each contractor at the contractor's site. Upon receipt of the equipment, the Scheduled Government-furnished Property List will be updated to include all such equipment. Contractor shall follow all Government property regulations as required by FAR 52.245-1, Government Property, Alternate I, and other applicable FAR and DFARS clauses as included in the contract. The Government will use an Engineering and Installation (E&I) Air National Guard squadron to transport GFP to the contractor's facility. The E&I squadron will rack and install the GFP at the contractor's facility. The transportation and installation of GFP will occur at no expense to the contractor. This subtask addresses CDRL B004.

3.5.1.1 Maintain equipment, ship and receive equipment, and maintain shipping, receiving, and accounting documentation (CDRL B004). Includes:

3.5.1.1.1 Prototype suite – rough description of the equipment, spell out purpose so it is clear what the GDSS PMO buys and what the using unit buys. Add in a ROM what the refresh rate is, who does the maintenance on it, and how the GFE is purchased.

3.5.1.1.2 Laptops and/or desktop computers – rough description of the equipment, to include make, model, characteristics, and purpose.

3.5.1.2 Provide inventory tracking, planning, and maintenance coordination.

3.5.1.3 Track maintenance and warranty status of GDSS equipment.

3.5.1.4 Maintain Government equipment accounts, Automated Data Processing Equipment (ADPE), in the Assets Inventory Management (AIM) in accordance with Air Force Instruction (AFI) 23-111 Management of Government Property in Possession of the Air Force, 7 Jan 2011 and Air Force Manual (AFMAN) 23-220 Reports of Survey for Air Force Property, 1 Jul 1996.

3.5.1.5 Individuals appointed to manage hardware shall comply with AFMAN17-1203, Information Technology (IT) Asset Management (ITAM), 19 Mar 2014.

3.5.1.6 Coordinate and maintain GDSS equipment.

3.5.1.7 Conduct Government property inventory annually or as requested by the COR.

3.5.1.8 Maintain familiarity with the Information Technology Asset Management (ITAM) Handbook.

3.5.1.9 Implement Asset Inventory methods to assist the COR in maintaining asset tracking and compliance with policy (CDRL B004).

3.5.2 Subtask 2 – Software. This subtask addresses CDRL B004.

3.5.2.1 The Contractor shall maintain software furnished by the Government, ship and receive software when required, and maintain software documentation, licenses, and copies. The Contractor shall maintain a comprehensive and readily available list of all software furnished by the Government to include license numbers,

product keys, and track all expirations if applicable (CDRL B004).

3.6 TASK 6 – Security Engineering Certification and Accreditation. The Contractor shall provide security engineering certification and accreditation by accomplishing the following tasks:

3.6.1 Subtask 1 – Certification and Accreditation Support. The Contractor shall provide security certification and accreditation support to GDSS PMO by providing the following services:

3.6.1.1 Provide the GDSS PMO inputs necessary to obtain and maintain the Authority to Operate (AtO), Authorization to Connect (AtC), Certificate of Networkiness (CoN), and Risk Management Framework (RMF) processes.

3.6.1.2 Advise and consult with the Program Manager on matters of information and system security.

3.6.1.3 Provide a mitigation recommendation to the COR within 24 hours after the RMF non-compliance became apparent to the Contractor.

3.6.1.4 Provide a recommendation to the COR to correct RMF non-compliance within 10 working days.

3.6.2 Subtask 2 – Vulnerability Management

3.6.2.1 The Contractor shall support PMO in responding to the United States Cyber Command (USCYBERCOM) Information Assurance Vulnerability Alert (IAVA), and keep abreast of Air Force Network Operations (AFNETOPS) Network Tasking Orders (NTO), and Notices to Airmen (NOTAMs), Security patches and Time Compliant Network Orders (TCNOs).

3.6.2.2 The Contractor shall support the development and maintenance of the GDSS Ports, Protocols and Services (PPS) Matrix to ensure proper registration with the Department of Defense and AFNETOPS.

3.6.3 Subtask 3 – GDSS Security and Documentation Support. This subtask addresses CDRL B005.

3.6.3.1 The Contractor shall provide to the COR reviews and reports on proposed changes to system hardware, software, or environment for impacts to the GDSS security posture and ensure changes do not violate the criteria for system accreditation (CDRL B005).

3.7 TASK 7 – Operations Support

3.7.1 Subtask 1 – Fielding Support. This task addresses CDRL C010. The Contractor shall provide the following (some of these subtasks must be accomplished in advance of fielding):

3.7.1.1 Research for new equipment specifications for upgrade efforts.

3.7.1.2 Inputs related to the GDSS installed sites and coordination of logistical support for existing and new sites.

3.7.1.3 Update GDSS Installation & Operations Document (CDRL C010).

3.7.2 Subtask 2 – Technical Support. This subtask addresses CDRLs B005, D002, D003, and E002. In accomplishing this task the Contractor shall provide the following to the PMO.

3.7.2.1 An initial response to queries within 60 minutes after receipt of verbal or written request.

3.7.2.2 Verbal notices reported to PMO within 60 minutes after the problem or the potential problem becomes apparent to the Contractor.

3.7.2.3 Proposal/recommendations for non-emergency situations shall be provided within 24 consecutive hours upon request from the COR. Proposal/recommendations for emergency situations shall be made IAW the Operational Readiness Criteria (provided at the time of award).

3.7.2.4 When there are situations requiring the Contractor to implement permanent corrective action, the Contractor shall institute, within 10 working days from implementing immediate corrective action, long term corrective action, as presented to the PMO (CDRL B005).

3.7.2.5 The Contractor shall provide on-call technical assistance with the GDSS application and associated specialized equipment. The Government shall have the ability to contact the contractor for on-call technical assistance 24x7x365. The Contractor shall provide advanced Level 3 GDSS software technical support for all GDSS environments when issues are elevated. This includes assisting with in-depth troubleshooting and fault isolation, providing technical expertise on all GDSS systems, repair and maintenance on preinstalled software.

3.7.2.6 Provide continuous on call engineering support. The Government shall have the ability to contact the contractor for on-call technical assistance 24x7x365. After normal work-hours, support can be through designated on-call person(s). Issue troubleshooting and resolution will continue until required by the Government.

3.7.2.7 Assist in fault/defect isolation analysis and resolution.

3.7.2.8 Document issues with the fielded system utilizing the Government-identified trouble reporting systems/methods (CDRL D002 and D003).

3.7.2.9 Coordinate all program system problem/outage resolutions with appropriate agencies or activities.

3.7.2.10 Provide assistance to resolve/fix problems.

3.7.2.11 Update the Government-provided problem reporting system within one hour after status change.

3.7.2.12 Generate SPRs (CDRL D002) for appropriate support actions to resolve problems requiring code changes.

3.7.2.13 Provide Technical Reports (CDRL B005) (white papers) to address proposed approach and technological changes.

3.7.2.14 Provide 24x7x365 troubleshooting assistance for all systems software components. The contractor shall provide Level 3 support which shall be performed wherever is necessary to ensure GDSS sustains a full operational capability.

3.7.2.15 Provide advanced Level 3 database administration support for troubleshooting assistance.

3.7.2.16 Within 5 work days, retrieve GDSS historical data that common users cannot obtain through normal means. Verify that the PMO has approved any users/requestors of the Historical Data to ensure proper identification of these individuals.

3.7.2.17 Develop, establish, and maintain the development environment matching the operational baseline (hardware & software). Any requests for deviation are to be submitted per the instructions provided in CDRL E002.

3.7.3 Subtask 3 – MEIS 3.3.3 Support (OPTIONAL). This subtask addresses MEIS 3.3.3 services and interfaces. The MEIS is the Service Oriented Architecture solution that provides cross-system services. The Contractor shall develop solutions to meet Government-directed changes and upgrades as required to sustain MEIS 3.3.3 and the MEIS GDSS Object Processor (MGOP). MEIS/MGOP support shall include Government-directed software changes as required for security, interface changes, business rule changes, etc. and Level 3

support as required for troubleshooting and resolution.

3.8 TASK 8 - Hardware

3.8.1 The Government may request the Contractor purchase specialized equipment as Other Direct Costs (ODCs). Requirements over the micro-purchase threshold as defined in FAR 2.101 must follow competition requirements and FAR/DFARS/AFFARS procedures and may result in contracting actions outside of this contract. After the requirements are determined, the COR will request the Contractor submit a proposed list to include quantities, delivery dates, and unit price of each item listed. The equipment list will be sent to the CO for approval and ensure funds are available. If there are any changes to the original proposal, the Contractor shall make a recommendation to the COR, and receive COR approval before purchasing any alternate. The Contractor shall inspect and test the equipment prior to invoicing for the equipment. If the equipment is damaged or does not operate according to its performance description, the Contractor shall return the nonconforming equipment for replacement or refund. ODCs will be reimbursed on a cost-reimbursable basis utilizing the ODC Contract Line Item Number (CLIN) established.

3.8.2 Configuration management of hardware shall include a comprehensive method of recording all hardware purchases made by the Contractor and warranty dates, support and warranty expiration dates, and a plan to provide adequate lead time to extend or replace warranties or support as needed.

3.8.3 Equipment Inventory Record (EIR): The Contractor shall prepare and maintain an equipment inventory record (CDRL B004).

The contractor shall provide an unalterable initial inventory within five work days after contract award to COR and report to the COR via marked-up inventory report and report any discrepancies between the list of Government property provided and the actual inventory. The Contractor shall:

- Update the EIR every 30 calendar days after completion of the initial inventory
- Provide the Government a fully reconciled EIR NLT 28 February of each year with the final EIR due NLT five days prior to contract completion.

The final EIR shall consist of the unalterable Government verified inventory and a duplicate in Excel that may be altered by the Government.

3.9 TASK 9 – Optional Additional MAJOR RELEASE

3.9.1 MAJOR RELEASE. The Government reserves the right to order one additional Major version release (GDSS Core) per each contract performance period. The Government exercising its rights under this task are subject to the availability of funds and approvals. The services to be provided under this task shall be identical to the instructions provided for Task 4, PWS Para. 3.4.7.2, et al.

4. Deliverables Management

All deliverables shall meet professional standards and meet the requirements set forth in contractual documentation. Unless otherwise specified, documents shall be delivered in electronic format using the Microsoft Office suite of applications and delivered to the AMC/A6IM GDSS PMO ensuring deliverables arrive in secure undamaged manner.

All deliverables are listed as DD Form 1423s Contract Data Requirements List and are reflected in the table below. One copy of the transmittal letter with the deliverable shall be provided to the COR through an assigned Email address or other method as agreed. All deliverables shall be in accordance with the instructions on the DD Form 1423. Deliverables, once submitted, cannot be revised but can be appended. All documentation generated becomes Government property.

Delivery days are calendar days unless otherwise started. If that date falls on a weekend, the delivery date will then be the following business day. All data deliverables shall be electronically delivered using Government provided data delivery system, unless instructed otherwise such as software deliveries.

Contract Data Requirements List (CDRL) Number	Deliverable Title	PWS Para
Plans and Agreements		
A001	Management Plan	3.1.2, 3.1.4, 3.1.4.3, 3.1.4.7
A002	Quality Program Plan	3.1.2, 3.4.5
A003	Technical & Management Work Plan	3.1.2, 3.1.3, 3.1.3.1, 3.1.4, 3.1.4.2, 3.1.4.4,
A004	Configuration Management Plan	3.1.2
A005	Software Development Plan	3.1.2, 5.1.2, 6.3.1,
Reports and Documents		
B001	Contract Performance Report (CPR)	3.1.2, 3.1.3, 3.1.3.1, 3.1.3.2, 6.3.2, 6.6.2
B002	Task Schedule Progress Review (TPR)	3.1.2, 3.1.3, 3.1.3.3,
B003	Integrated Master Schedule	3.1.2, 3.1.3, 3.1.3.1, 3.1.4, 3.1.4.1, 3.1.4.5, 3.1.4.6,
B004	Equipment Inventory Record (EIR)	3.1.2, 3.5.1, 3.5.1.1, 3.5.1.9, 3.5.2, 3.5.2.1, 3.8.3, 8.2.2, 8.3.11,
B005	Scientific & Technical Reports	3.1.2, 3.1.3, 3.1.3.5, 3.2.1, 3.2.1.6, 3.1.3, 3.4.2, 3.4.6, 3.4.6.1, 3.4.8, 3.4.8.1, 3.4.8.2, 3.4.8.4, 3.4.8.5, 3.4.8.7, 3.4.12,

Contract Data Requirements List (CDRL) Number	Deliverable Title	PWS Para
		3.4.12.12.1, 3.6.3, 3.6.3.1, 3.7.2, 3.7.2.4, 3.7.2.13
B006	Software Test Report (STR)/ Software Test Description	3.1.2, 3.2.1, 3.2.1.6, 3.4.14, 3.4.14.7
B007	Agenda/ Minutes	3.1.2, 3.1.3, 3.1.3.1, 3.1.3.5, 3.2.1, 3.2.1.6,
B008	Test Readiness Review	3.1.2, 3.4.14, 3.4.14.2
B009	Contract Work Breakdown Structure	3.1.2, 6.3.1, 6.3.3
Procedures and Descriptions		
C001	Test Procedures/ Cases	3.1.2, 3.2.1, 3.2.1.1, 3.2.1.6, 3.4.12, 3.4.12.5, 3.4.14, 3.4.14.1
C002	Interface Requirements Specification (IRS)	3.1.2, 3.4.9, 3.4.9.1
C003	Interface Design Description (IDD)	3.1.2, 3.4.9, 3.4.9.1
C004	Database Design Description	3.1.2, 3.4.9, 3.4.9.1
C005	Software Design Description	3.1.2, 3.4.9, 3.4.9.1
C006	Software Version Description	3.1.2, 3.4.8, 3.4.8.4, 3.4.8.6, 3.4.9, 3.4.9.1,
C007	Software User's Manual (SUM) (Including GDSS User's Manual (GUM))	3.1.2, 3.4.16, 3.4.16.1,
C008	System/ Subsystem Design Description	3.1.2, 3.4.6, 3.4.6.1, 3.4.9, 3.4.9.1

Contract Data Requirements List (CDRL) Number	Deliverable Title	PWS Para
C009	Computer Software End Items	3.1.2, 3.2.1.1, 3.4.7, 3.4.7.2, 3.4.7.3, 3.4.12, 3.4.12.5, 3.4.17, 3.4.17.1
C010	GDSS Installation & Operations Document	3.1.2, 3.2.1.1, 3.4.12, 3.4.12.5, 3.4.17, 3.4.17.6, 3.7.1, 3.7.1.3
C011	Difference Document/ What's New Document	3.1.2, 3.2.1, 3.2.1.6, 3.4.12, 3.4.12.5, 3.4.16, 5.1.2
C012	Requirements Specification Agreement (RSA)	3.1.2, 3.4.8, 3.4.8.4, 3.4.8.6
Change Requests		
D001	Baseline Change Request (BCR)	3.1.2, 3.4.8, 3.4.8.3
D002	Software Problem Report (SPR)	3.1.2, 3.4.8, 3.4.8.3, 3.7.2, 3.7.2.8, 3.7.2.12
D003	Document Change Request (DCR)	3.1.2, 3.4.8, 3.4.8.3, 3.7.2, 3.7.2.8
Other		
E001	Engineering Change Proposal	3.1.2, 3.4.5, 3.4.6.1, 3.4.8, 3.4.8.1, 3.4.12.12.1
E002	Request For Deviation	3.1.2, 3.7.2, 3.7.2.17
E003	Training Conduct Support Document (TCSD)/ Training Lesson (TL)	3.1.2, 3.2.1, 3.2.1.3, 3.2.1.3.1, 3.2.1.4

5.0 SERVICES SUMMARY

5.1 SPECIFIC STANDARDS

5.1.1 The Services Summary table below summarizes the most important performance objectives and

performance thresholds (specific standards) as identified within the body of the PWS. The absence of any performance objective and threshold from this Services Summary shall not detract from its enforceability nor limit the rights or remedies of the Government under any provision of the contract. Metrics shall be calculated monthly except for Service Oriented C2 Sustainment. The Service Delivery Summary will be in accordance with AFI 63-101/20-101, Integrated Life Cycle Management 16 September 2016, AFI 10-601, Operational Capability Requirements Development and FAR Subpart 37.6, Performance-Based Acquisition.

5.1.2 Table 2 - Specific Standards

Performance Objective	PWS Para.	Performance Threshold	Metric	Method of Surveillance
Plans and Agreements Documentation (CDRLs A001, A002, A003, A004, and A005) provided is clear, complete, and consistent, and contains the appropriate level of supporting information.	3.1.2	No more than one rewrite resulting from inaccurate, incomplete, or unsupported information per submitted document. In the case of documents requiring updates, no more than one rewrite resulting from inaccurate, incomplete, or unsupported information per updated document.	Number of rewrites resulting from inaccurate, incomplete, or unsupported information.	100% Inspection
Reports and Documents Agendas/Minutes (CDRL B007) documentation provided is accurate, and contains the appropriate level of detail.	3.1.2, 3.1.3, 3.1.3.1, 3.1.3.5, 3.2.1, 3.2.1.6	No more than three rewrites per quarter resulting from inaccurate, incomplete, or unsupported information.	Number of rewrites resulting from inaccurate, incomplete, or unsupported information.	Random Sampling
All reports and Documents (CDRL BXXX) except Agendas/Minutes (CDRL B007) documentation provided is accurate, and contains the	3.1.2, 3.1.3, 3.1.3.1, 3.1.3.5, 3.2.1, 3.2.1.6	No more than one rewrite per month resulting from inaccurate, incomplete, or unsupported information.	Number of rewrites resulting from inaccurate, incomplete, or unsupported information.	100% Inspection

Performance Objective	PWS Para.	Performance Threshold	Metric	Method of Surveillance
appropriate level of detail.				
All Procedures and Description technical documentation (CDRL C001, C002, C003, C004, C005, C006, C007, C008, C010, C011, and C012) provided is accurate, and contains the appropriate level of detail.	3.1.2,4	No more than one adverse incident per quarter in handling the software, leading to system problems or failures will not be a result of errors or misdirection in the documentation. No more than three rewrites per quarter resulting from inaccurate, incomplete, or unsupported information.	Number of adverse incidents caused by document errors. Number of rewrites resulting from inaccurate, incomplete, or unsupported information.	100% Inspection
All Procedures and Description Computer Software End Items (C009) provided are free from critical errors.	3.1.2, 4	No more than eight re-deliveries of CCB code fixes per quarter. No more than three Must Fix test findings per major release.	Number of re-deliveries of CCB code fixes due to coding errors or associated included documentation. Number of Must Fix test findings discovered during Government testing.	100% Inspection
All Change Request (D001, D002, D003) and Other (E001, E002, E003) documentation provided is accurate, and contains the appropriate level of detail.	3.1.2, 4	No more than three rewrites per quarter resulting from inaccurate, incomplete, or unsupported information.	Number of rewrites resulting from inaccurate, incomplete, or unsupported information.	100% Inspection
Data deliverables are produced using prescribed formats, software tools, and	3.12, 4	No more than two inaccuracies per month for cross-referencing	Number of inaccuracies for cross-referencing source and reference material content.	Random Sampling

Performance Objective	PWS Para.	Performance Threshold	Metric	Method of Surveillance
software versions as agreed to by the COR. All deliverables meet professional standards for technical writing and the requirements set forth in the contract. All deliverables clearly identify assumptions and personal opinions. Technical writing and reports are delivered to the COR by the agreed to schedule or in accordance with the terms of the contract.		source and reference material content. No more than one late deliverable per month. No late deliverables per month submitted more than one working day beyond the agreed-to time period.	Number of late deliverables. Number of late deliverables submitted more than one working day beyond the agreed-to time period.	
Level of expertise, coordination, and support necessary to accomplish the contract in a responsive, satisfactory, and timely manner is provided.	3, 3.7	No more than one formal customer complaint per month in performance of required tasks. No complaints left unresolved one working day beyond the agreed-to time period per month.	Number of formal customer complaints. Number of complaints left unresolved one working day beyond the agreed-to time period.	Customer Complaint Record
Effective corrective actions ensure noted discrepancies are corrected, COR follow-ups are precluded, and corrective actions eliminate recurrence of the same or similar discrepancies.	3.4.,	All deficiencies are corrected not later than one working day beyond the agreed-to time period per month.	Number of deficiencies not corrected one working day beyond the agreed-to time period.	Random Sampling

Performance Objective	PWS Para.	Performance Threshold	Metric	Method of Surveillance
Initial responses to the PMO for technical support are provided timely.	3.4.8, 3.7.2.1	Initial responses provided to the PMO within one hour after receipt of a verbal or written request. No instances of late initial responses per month.	Number of late initial responses.	100% Inspection
Verbal notice to the PMO of actual or potential problems is reported timely.	3.7.2.2	Verbal notices reported to the PMO within one hour after the problem or the potential problem becomes apparent to the Contractor. No instances of late verbal notices per month.	Number of late verbal notices.	100% Inspection
Proposals for non-emergency immediate corrective action are provided to the PMO timely.	3.7.2.3	Proposals provided to the PMO within 24 hours. No instances of late proposals per month.	Number of late proposals.	100% Inspection
The contractor shall, in writing, report to the CO with prompt and full disclosure of the Conflict of Interest incident or incidents	6.8	Contractor shall have no incidents of not providing prompt and full disclosure of Conflict of Interest per month.	Report of Conflict of Interest situations provided by Government or Contractor personnel or third parties.	100% Inspection

6.0 GENERAL INFORMATION / PERIOD OF PERFORMANCE

The total period of performance (POP) is a 90 day phase-in period followed by a 9-month base period, with four 12-month option periods, and an optional 6-month Extension of Service (EoS).

6.1 PROGRAM DATA

6.1.1 Program Contact Information

6.1.1.1 The PMO for GDSS is located at Scott AFB. Specific contact information will be restricted before award of this contract; communications shall only be through the CO until award.

6.1.2 Program Categories/Phase

6.1.2.1 GDSS is transitioning from Department of Defense Information Assurance Certification and Accreditation Process (DIACAP) to Risk Management Framework (RMF). This transition shifts focus away from traditional Mission Assurance Category (MAC) levels to Confidentiality, Integrity, Availability (CIA) security categorization. GDSS, a MAC-1 system under DIACAP, has been categorized as a Low/High/High (for its unclassified instance) and Moderate/High/High (for its classified instance) system under RMF. This CIA determination enables GDSS to proactively implement appropriate information security controls and in turn support the mission in a cost-effective manner. The system continues to handle information vital to the operational readiness or effectiveness of deployed or contingency forces. The loss of data would cause severe damage to the successful completion of a DOD mission, meaning the system must maintain the highest levels of both integrity and availability and use the most rigorous measure of protection.

The loss of confidentiality (unclassified, low) for GDSS could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals. A limited adverse effect means that, for example, the loss of confidentiality might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.

The loss of confidentiality (classified, moderate) could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. A serious adverse effect means that, for example, the loss of confidentiality might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.

The loss of integrity or availability (high) for GDSS could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals. A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.

6.1.2.2 Acquisition Category. GDSS is an Acquisition Category (ACAT) III program as defined in the ORD AMC003-81A approved by Air Force Requirements Oversight Council (AFROC) 11-02-05, 14 November 2002.

6.1.2.3 DITPR Status. GDSS is a system of record in the DOD Defense Information Technology Portfolio Repository (DITPR). The GDSS program is registered in the DITPR, Identification Number 370.

6.1.2.4 Acquisition Phase. The following diagram defines the current status of GDSS in the acquisition phase, in compliance with AFI 10-601, Operational Capability Requirements Development, 12 July 2010.

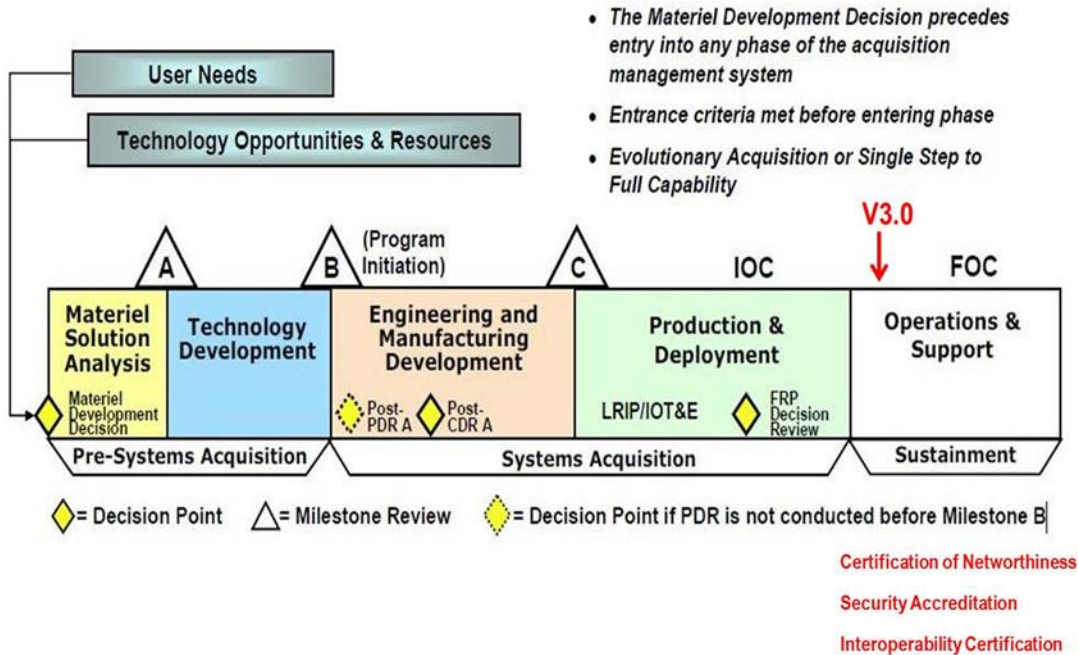


Figure 1-8: GDSS Acquisition Framework Status

6.1.2.5 Present Milestone. GDSS has reached Post Milestone C, Full Operational Capability (FOC), sustainment phase. Mission demands make it is necessary to maintain GDSS in a mixed cycle of development and maintenance, and is reported to U.S. Office of Management and Budget (OMB) in this category.

6.1.2.6 Projected Milestone Date. GDSS is already post milestone C, the projected year for sundown of this system is estimated to be 2026.

6.2 VERSION RELEASE THEMES

6.2.1 Version 3.X

6.2.1.1 Version 3.X is the current version in sustainment. This sustainment effort is to provide GDSS software modification for interface changes and software obsolescence to keep pace with associated COTS and DOD systems as well as maintaining compliance with DOD security measures on NIPRNet and SIPRNet systems, AvORM software sustainment, and sustain multi-level cross security domain.

6.2.1.2 Continue investigation of transitioning selected functionality to stand alone applications on the enterprise SOA.

6.2.1.2.1 Continue to utilize a hybrid of traditional and “Agile Development” techniques to deliver software more focused on user needs and processes in a more timely fashion.

6.3 WORK BREAKDOWN STRUCTURE/EARNED VALUE MANAGEMENT

6.3.1 The Contractor shall establish, integrate, and report the program-wide Work Breakdown Structure (WBS) to lower level WBS, as depicted in Figure 5-1, below (CDRL B009). The Contractor shall maintain sufficient detail within the WBS to support the Program’s migration to Performance-Based Management and shall support the Program’s efforts in tracking and maintaining the Integrated Master Schedule within Project Server. The WBS shall align with the tasks described in this PWS and as described in MIL-HDBK-881,

Department of Defense Handbook Work Breakdown Structure, which may further be defined or modified by the Program (CDRL A005).

6.3.2 Earned Value Management (EVM) addresses CDRL B001. EVM is a program management tool that integrates the technical, cost, and schedule parameters of a project into a Performance Measurement Baseline (PMB). It measures how efficiently resources are consumed against what was planned to be consumed to meet technical goals. The Contractor shall use EVM as a management tool and provide EVM data to the PM (B001). The Contractor has ownership of the Earned Value Management System (EVMS), and is expected to maintain compliance with the EVMS standard and uses EVM as an internal management tool. EVM shall be incorporated into the Integrated Master Schedule.

Figure 5-1: Work Breakdown Structure

Level 1	Level 2	Level 3	Level 4	Level 5
Program	Major Function	Release or Sub-function Cost	Sub-function Cost	Contractor-defined
3. GDSS				
	3.1 Enterprise IT Policy and Planning			
		3.1.2 Documents		
		3.1.3 Support and Attend Meetings and Conferences		
			3.1.3.2 Contractor Performance Review	
			3.1.3.4 Lead Agile Teams	
		3.1.4 Task Schedule Progress Review		
	3.2 Integrated Solutions Management			
		3.2.1 Systems Integration		
		3.2.2 Additional Integration Efforts		

	3.3 Market Research and Prototyping			
	3.4 Custom Application Development			
		3.4.4 Configuration Management		
		3.4.5 Quality Control		
		3.4.6 Interoperability and Architecture Support		
		3.4.7 Software Release Process		
			3.4.7.1 Frequency of Releases	
		3.4.8 Analyze		
			3.4.8.1 ROM	
		3.4.9 Design		
		3.4.12 Develop		
			3.4.12.11 Opportune Fixes	
			3.4.12.12 Innovations	
		3.4.13 Emerging Technology Integration		
		3.4.14 Test		
		3.4.17 Deliver		
	3.5 Asset Management			

		3.5.1 Govt Furnished Equipment		
		3.5.2 Software		
	3.6 Security Engineering Certification and Accreditation			
		3.6.1 Certification and Accreditation Support		
		3.6.2 Vulnerability Management		
		3.6.3 GDSS Security and Documentation Support		
	3.7 Operations Support			
		3.7.1 Fielding Support		
		3.7.2 Technical Support		
			3.7.2.5 24x7 Technical Assistance	
			3.7.2.12-13 SPRs and Technical Reports	
	3.8 Hardware			
		3.8.1 Configuration Management		
	7.3.1 Security Manangement/ Personnel Security			
	7.4 Program Management Assistance			

		7.4.2 Safeguard Classified		
	7.5 Contractor Access			
		7.5.1 Badges		
	7.10 Contractor Personnel Training			
		7.10.1 IA Training		
		7.10.1 8570 Training		

6.3.3 Blocks 10, 12, and 13 – DI-MGMT-18334 requires the first submissions to be made IAW CDRL B009. The contractor is responsible for maintaining the CWBS Dictionary during the life of the contract. Subsequent dates of submission shall be made as required or upon major revisions. CWBS Dictionary submissions shall not be more frequent than report submission.

6.3.4 Prepare the CWBS in accordance with MIL-HDBK-881, "Work Breakdown Structures for Material Items" and DI-MGMT 81334 (most recently approved version). For Cost and Software Data Reporting (CSDR) purposes, the CWBS must be prepared in accordance with the CSDR Manual (DOD 500.4-M-1) and the contract CSDR Plan approved by the Cost Analysis Improvement Group (CAIG) Chair. The CSDR Manual is available from the Defense cost and Resource Center (DCARC) Website at <http://dcarc.pae.osd.mil>.

6.3.5 The CWBS and Dictionary must be electronically forwarded to the DCARC Website at <http://dcarc.pae.osd.mil>. Prime contractors shall flow-down CSDR requirements contained in their prime contracts to all their subcontractors who meet the reporting thresholds. This includes requiring subcontractors to electronically report directly to the DCARC.

6.4 PLACE OF PERFORMANCE

6.4.1 The services described in paragraphs 3.6.2, 3.2.1.5, 6.5.1.2, and 8.0 contain circumstances where the Contractor shall provide services at Scott AFB, IL. All other tasks shall be performed at the Contractor's site and from time-to-time at other locations designated by the COR.

6.4.2 The COR may require the Contractor to provide these services from a Government furnished facility. The COR, in this case, will provide the maximum amount of lead-time to the Contractor before initiating any direction to transfer place of performance changes that impact the contract.

6.4.3 All meetings, reviews, and audits will be held at Scott AFB or the local Contractor facilities, except when alternate locations are agreed upon by the Contractor and the COR. Management, technical studies, analysis, and associated activities may be conducted at the most feasible and economical location.

6.5 DUTY HOURS

6.5.1.1 Maintenance of GDSS consists of two different types of duty hours.

6.5.1.2 Technical support availability shall be 24x7x365. Contractor shall be available to correspond and attend meetings with the Government during normal duty hours. Government duty hours are 0730-1630 hours Monday

through Friday, except for Federal holidays. Other services/tasks shall be based on the delivery schedules of due-ins/deliverables, meeting schedules.

6.6 TRAVEL

6.6.1 Travel by Contractor personnel may be required in support of this contract. The Contractor shall obtain approval for need of travel by the COR prior to travel commencement. Additionally, the Contractor shall receive CO confirmation on availability of funds prior to traveling. Reimbursement for travel outside the local area is authorized in support of this contract. Travel shall be reimbursed at cost in IAW with FAR 31.205-46.

6.6.2 The Contractor shall submit a travel itinerary and estimated cost for approval by the COR and confirmation on availability of funds from the CO not later than five workdays prior to travel. The COR will confirm the need for travel, and the CO will confirm the availability of funds prior to travel. Per Diem and travel rates shall not exceed the amount authorized. Airfare shall be the prevailing rates for commercial airlines at coach class. All travel arrangements shall be the responsibility of the Contractor, to include airfare reservations, lodging reservations, and rental car reservations. The Contractor should make all effort to schedule travel far enough in advance to take advantage of reduced airfares. When required, the most reasonable means of ground transportation (i.e. taxi, bus, rental car) shall also be used. The Government shall not reimburse local travel (defined as any travel 50 miles or less one-way) and related expenses to the Contractor for daily travel to or from work at Scott AFB, IL. The Contractor shall monitor all non-local expenditure and provide expense status to the COR in the monthly Contract Program and Status Review (CDRL B001). CONUS and OCONUS travel, including travel to the AOR, will be required under this contract. Travel will be reimbursed at allowable cost in accordance with the Federal Acquisition Regulation (FAR) 31.205-46, Travel Costs, in effect on the date(s) the travel is performed. Five workdays after conclusion of the trip, a trip report will be submitted to the COR for approval.

6.7 DATA RIGHTS

6.7.1 Pursuant to DFARS 252.227-7014(b)(1) The Contractor shall grant the Government unlimited rights to all computer software and/or computer software developed during the performance of the contract. The unlimited rights license granted to the Government shall include the Government having sole use and unlimited use and distribution rights to the software and software documentation developed under the contract, whether or not the software and software documentation are listed deliverables under the contract.

6.7.2 Pursuant to DFARS 252.227-7014(e) The Contractor shall complete and submit the following as attachment to its proposal: The Contractor asserts for itself, or the persons identified below, that the Government's rights to use, release, or disclose the following computer software should be restricted:

Computer Software			Name of Person
to be Furnished	Basis for	Asserted Rights	Asserting
With Restrictions*	Assertion**	Category***	Restrictions****
(LIST)	(LIST)	(LIST)	(LIST)

*Generally, development at private expense, either exclusively or partially, is the only basis for asserting restrictions on the Government's rights to use, release, or disclose computer software.

**Indicate whether development was exclusively or partially at private expense. If development was not at private expense, enter the specific reason for asserting that the Government's rights should be restricted.

***Enter asserted rights category (e.g., restricted or Government purpose rights in computer software, Government purpose license rights from a prior contract, rights in SBIR software generated under another contract, or specifically negotiated licenses).

****Corporation, individual, or other person, as appropriate.

Date _____

Printed Name and Title _____

Signature _____

(End of identification and assertion)

If the software is not listed in the attachment, any claims by the Contractor that the software and/or software documentation is proprietary, trade secret, or otherwise restricts the Government's unlimited and sole use and unlimited distribution rights shall be forfeited by the Contractor. In addition the Contractor shall automatically deliver, at the completion of the contract or as otherwise directed, to the Government the software and software documentation and vest in the Government unlimited and sole use and unlimited distribution rights to the software and/or software documentation.

6.8 ORGANIZATIONAL CONFLICT OF INTEREST (OCI)

6.8.1 For general information on the handling of Organizational Conflict of Interest (OCI), reference Federal Acquisition Regulation (FAR) 9.5.

6.8.2 Identification and Mitigation Plan. The contractor must maintain an OCI Identification and Mitigation Plan (OIMP) acceptable to the CO. The OIMP shall include, among other information, processes and internal controls necessary to identify, capture, and mitigate OCI activities at the subcontractor level.

6.8.3 Mitigation Plan Revision. The contractor must provide a draft revision of its plan to the CO 30 days prior to any anticipated change, and such change must be negotiated and incorporated into the contract prior to implementation of a change.

6.8.4 Violation Reporting. When the contractor discovers an OCI, potential OCI, or violation of the OIMP with respect to this contract, either by its own employee or that of one of its subcontractors, the contractor shall in writing report to the CO with prompt and full disclosure of the incident or incidents. The report shall include a description of the OCI violation and proposed contractor actions to avoid, neutralize, or mitigate and/or preclude repetition of the violation. After conducting necessary inquiries and discussions, the CO and the contractor shall agree on appropriate action, or the CO shall take such action afforded under the terms of the contract and statute, to include updating the OIMP.

6.9 CONTRACTOR MANPOWER REPORTING

6.9.1 The contractor shall report ALL contractor labor hours (including subcontractor labor hours) required for performance of services provided under this contract for the GDSS Service Oriented C2 Sustainment via a secure data collection site. The contractor is required to completely fill in all required data fields at <http://www.ecmra.mil>.

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

6.10 NON-PERSONAL SERVICES

The Government will neither supervise contractor employees nor control the method by which the contractor performs the required tasks. Under no circumstances shall the Government assign tasks to, or prepare work schedules for, individual contractor employees. It shall be the responsibility of the contractor to manage its employees and to guard against any actions that are of the nature of personal services, or give the perception of personal services. If the contractor feels that any actions constitute, or are perceived to constitute personal services, it shall be the contractor's responsibility to notify the TO Contracting Officers (CO) immediately. These services shall not be used to perform work of a policy/decision making or management nature, i.e. inherently Governmental functions. All decisions relative to programs supported by the contractor shall be the sole responsibility of the Government. These operating procedures may be superseded by Theater Commander's direction during deployments.

6.11 CONTRACTOR IDENTIFICATION

6.11.1 Identification Badges

The Contractor is required to provide identification badges for their employees. All Contractor personnel shall wear these badges while on duty on the Government site. Badges are required to identify the individual, company name, and be clearly and distinctly marked as Contractor. Size, color, style, etc. are to be mutually agreed to by Contractor and COR. The Contractor's identification badge will not be used as an entry requirement for installation entry or into any Government designated controlled or restricted area.

6.11.2 Identification in the Workplace

When conversing with Government personnel during business meetings, over the telephone or via electronic mail, contractors/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, contractors/subcontractors occupying collocated space with their Government program customer should identify their work space area with their name and company affiliation.

6.11.3 Performance Reporting

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

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

6.12 Program Management / Project Management

The Contractor shall identify a Program Manager or a Project Manager who shall be the primary representative responsible for all work awarded under this contract, participating in Program/Project Management Reviews and ensuring all standards referenced herein are adhered to.

6.13 Contract Management

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

6.14 Documentation and Data Management

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

6.15 Records, Files, and Documents

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

7.0 SECURITY

The Contractor shall not employ persons to perform under this contract if such employee is deemed or identified by Scott AFB as a potential threat to the health, safety, security, general well-being or operational mission of the installation and its population, nor shall the Contractor or Subcontractor employ persons under this contract who have an outstanding criminal warrant as identified by Law Enforcement Agency Data System (LEADS) through the National Crime Information Center. LEADS checks will verify if a person is wanted by local, state, and federal agencies. All Contractor and Subcontractor personnel must consent to LEADS background checks. Contractor and Subcontractor personnel who do not consent to a LEADS check will be denied access to the installation. Information required to conduct a LEADS check includes: full name, driver's license number, and/or social security number, date of birth of the person entering the installation, and completion of a background check questionnaire. The Contractor must have this information ready to provide to the installation's Visitor Control Center, if requested.

The Contractor shall not be entitled to any compensation for delays or expenses associated with complying with the provisions of this clause. Furthermore, nothing in this clause shall excuse the Contractor from proceeding with the contract as required.

7.1 CLASSIFICATION LEVEL

7.1.1 The highest security classification required by this contract is SECRET. Required Contractor personnel shall possess appropriate security clearances as of contract award date. The Contractor shall be given access to applicable documentation to include requirements, plans, specifications, studies, and analyses up to and including SECRET classification. The contract and its attachments are unclassified. DD Form 254 Department of Defense Contract Security Classification Specification provides security classification requirements to the Contractor. The Contractor shall comply with applicable instructions provided in the DD Form 254 and DOD/Air Force security regulations when handling classified material.

7.2 ACCESS TO GOVERNMENT SYSTEMS AND TO INSTALLATION DURING FORCE PROTECTION CONDITIONS (FPCONs)

7.2.1 Contractors requiring access to Government Automated Information Systems (AIS) shall have background investigations and security awareness training completed prior to the start of contract performance or immediately after being hired or transferred. All Contractor and subcontractor personnel shall have the appropriate security clearance before being authorized access to federal Government computers and networks. Contractor personnel shall comply with all AMC security requirements pursuant to DODI 5200.2, DOD Personnel Security Program, which requires DOD military, and civilian personnel, as well as DOD consultant and Contractor personnel who perform work on sensitive AIS to be assigned to positions which are designated sensitive. All personnel must complete Annual Information Assurance training via online CBT (<https://amc.csd.disa.mil/>). All personnel must comply with DOD 8570.01-M, Information Assurance Workforce Improvement Program and must provide certifications prior to contract start date. Contractor employees assigned to performing functional services duties, which include Account Management and System Administration shall meet and maintain DOD 8570.01-M certification Information Assurance Technical (IAT) Level I, A+ certification or Government-approved equivalent by full performance start date. Contractor employees assigned to performing CSA duties, and any contract lead shall meet and maintain DOD 8570.01-M certification IAT Level II certification by full performance start date.

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

7.2.3 The Contractor must comply with security regulations imposed by the installation commander and/or the agency responsible for the project location. Due to specific mission requirements inherent in the nature of controlled or restricted areas on the installation, the Government may direct the Contractor to leave the controlled or restricted areas at any given time. If this direction increases the cost of or the time required to complete the work, the contract price or schedule, or both must be adjusted accordingly through a modification to the contract.

7.2.4 When the period of performance is complete or Contractor personnel leave work on this project, they shall have five days to terminate all network user accounts and to return all CAC cards and base identification badges to the Government Trusted Agent. The Contractor shall maintain security requirements required for Government access and certification.

7.3.1 SECURITY MANAGEMENT / PERSONNEL SECURITY

7.3.2 The Contractor shall oversee security concerns, identifying conflicts/concerns and solutions, and implement procedures to maintain control and auditing of security for its personnel, its data, and its computer system access. The Contractor shall ensure that all work remains compliant with all applicable Air Force Security Regulations and security levels.

7.3.3 All services provided must be consistent with Air Force policy, rules, regulations, instructions, orders, guidance, and practices.

7.4 PROGRAM MANAGEMENT ASSISTANCE

7.4.1 The GDSS Program Management Office, HQ AMC/A6IM, or its successor organization, shall assist Contractor personnel in processing the necessary DOD forms to obtain base or area badges for access to Government facilities.

7.4.2 The Contractor shall provide for the handling and safeguarding of all classified information in accordance with AF Standards for storing, processing, and handling classified information and systems. Contractor personnel shall have the appropriate security clearance for the facilities in which the work is required.

7.5 CONTRACTOR ACCESS

7.5.1 Badges: Contractor shall comply with Scott Air Force Base's or other federal Government facility's Contractor identification procedures, including identification of Contractor status at meetings. Contractor personnel shall comply with all Government facility rules, regulations, and security requirements when entering, visiting, or leaving the base. These rules, regulations, and security requirements include the following: presenting valid identification for base entrance, obeying all posted directives, and providing strict adherence to Security Forces direction in instances where Security Forces have been dispatched to a particular location. The Contractor is required to provide identification badges for their employees. All Contractor personnel shall wear these badges while on duty on the Government site. Badges are required to identify (including photograph) the individual, company name, and be clearly and distinctly marked as Contractor.

7.5.1.1 Individual Contractors removed from this contract for any reason will be required to turn in their access badge immediately to Government in the Program Management Office.

7.5.2 Non-Disclosure Agreements: The Contractor shall execute non-disclosure agreements before the Contractor obtains or is provided Government "For Official Use Only" and classified information, regardless of source. In performance of this contract, the Contractor may obtain access to sensitive, nonpublic information. The Contractor agrees (a) to use and protect such information from unauthorized disclosure in accordance with the FAR; (b) to use and disclose such information only for the purpose of performing this contract and to not use or disclose such information for any personal or commercial purpose; (c) to obtain permission of the COR before disclosing/discussing such information with a third party; (d) to return, upon Government request, any non-public, sensitive information no longer required for Contractor performance; and (e) to advise the Government of any unauthorized release of such information. Upon request, the Contractor shall have its employees assigned to this contract execute a non-disclosure agreement for delivery to the Government. The Government shall require Contractor personnel both on and off-site to sign a non-disclosure statement to protect non-public information of the Government (reference Attachment 2). The Contractor shall maintain the nondisclosure agreements and have these agreements available for COR review during the life of the contract. At the end of the contract, the Contractor shall turnover to the COR, its personnel non-disclosure agreements.

7.6 ACCESS TO GOVERNMENT FACILITIES

7.6.1 The Government, based on assessment of the Contractor's need, shall provide the Contractor access to GDSS program facilities from the commencement of the contract until contract completion. Only Contractor (or subcontractor) personnel possessing the proper clearance will be authorized entry to restricted areas. All Contractor personnel must either have the appropriate building access permissions and ID cards or otherwise must be continuously escorted by Government approved personnel.

7.6.2 Property Protection. Property protection for the facility where contractor's primary work center is located will be the responsibility of the local facility manager and local government Security Manager, or their duly authorized representative IAW AFI 31-101, Integrated Defense (FOUO), and command/local directives. Contractor must safeguard all government-owned equipment and materials in his/her possession or use.

7.6.3 Contractor Working in Controlled or Restricted Areas. In the unlikely event that a contractor requires access to the controlled or restricted area and does not have the proper security clearance, government will ensure escort(s) are provided for contractor at all times when within a controlled or restricted area. Based on AMC procedures, contractor may act as escort officials under certain circumstances. Contractor must have an issued AF

Form 1199 and work on base a minimum of four days a week (must have an assigned workspace on base). Contractor is only allowed to escort visitors from the same company for which he/she works, and all visits must be for official business. In addition, contractor must fulfill, maintain, and comply with all security requirements IAW Integrated Defense and command/local directives. Contractor must comply with security regulations imposed by the installation commander and/or the agency responsible for the project location. Due to specific mission requirements inherent in the nature of controlled or restricted areas on Air Force installations, Government may direct Contractor to leave the controlled or restricted area at any given time.

7.6.4 Access to Government Facilities with Controlled or Restricted Areas. Contractor shall comply with security regulations imposed by the installation commander and/or the agency responsible for the project location. Due to specific mission requirements inherent in the nature of controlled or restricted areas on Scott AFB, government may direct contractor to leave the controlled or restricted areas at any given time.

7.6.5 Access to Government Facilities with Controlled or Restricted Areas for Replacement Contractor. The following scenario (i.e., replacement contractor with an inadequate security clearance) is abnormal. Government will ensure replacement contractors not initially possessing the proper clearances and requiring entry to controlled or restricted areas are escorted continuously. Replacement contractor must submit paperwork within seven days of being assigned to obtain an approved security clearance or favorable review. Replacement contractor personnel must obtain a security clearance prior to working with, or having direct access to, classified material. In addition, replacement contractor personnel must obtain a "favorable review" prior to having access to a Controlled Area. The above information must be submitted to 375 SFS/S5 or as directed by Government.

7.7 PROTECTION OF SYSTEM DATA / SITE SECURITY

7.7.1 Unless otherwise stated in the contract, the Contractor shall protect system design-related documents and operational data whether in written form or in electronic form via a network in accordance with all applicable policies and procedures for such data, including DOD Regulation 5400.07 and DOD Manual 5200.01(v1-v4), DOD Information Security Program: Overview, Classification, and Declassification, to include latest changes, and applicable service/agency/ combatant command policies and procedures. The Contractor shall protect system design related documents and operational data at least to the level provided by Secure Sockets Layer (SSL)/Transport Security Layer (TSL)-protected web site connections with certificate and or user ID/password-based access controls. In either case, the certificates used by the Contractor for these protections shall be DOD or IC approved Public Key Infrastructure (PKI) certificates issued by a DOD or IC approved External Certification Authority (ECA) and shall make use of at least 128-bit encryption.

7.7.2 Responsibility for the Contractor's compliance with internal security at a GDSS Program node shall be assigned the Contractor. All Contractor personnel shall be briefed on site security operating procedures upon commencement of contract award and shall be debriefed upon termination. The Contractor shall be responsible for all continuing security training of the Contractor, subcontractor, and any associate Contractor personnel.

7.8 SYSTEM ENGINEERING

7.8.1 US Air Force Standard Desktop Configuration (SDC)

All services provided under this Contract shall function under the fielded SDCs and be in compliance with AFMAN17-100, Air Force Information Technology (IT) Service Management, 16 Sep 2014), i.e. not altering the Air Force SDC.

7.9 NETWORK, COMPUTER, and INFORMATION SECURITY

7.9.1 Information given to the Contractor during the life of this contract shall only be used for the purpose of carrying out the provisions of this contract. The Contractor shall ensure it is knowledgeable with AFI 33-200 and AMC system security policies, and ensure the software it delivers to the COR is compliant with those policies.

7.9.2 FOUO: Agency information marked "For Official Use Only" (FOUO) or bearing other sensitivity markings shall be handled in accordance with agency information security program regulations and instructions

provided on the DD Form 254. This information shall not be divulged or disclosed without agency permission. Requests for disclosure shall be addressed to Government. Contractor personnel shall ensure information that is considered sensitive or proprietary is not compromised.

7.9.3 Privacy Act: Work on this project requires that personnel have access to Privacy Information (PII). PII shall be safeguarded in compliance with Federal/DOD PII guidelines, Title 5 U.S.C 552a "Records Maintained on Individuals," DOD Publication 5400.11-R "Department of Defense Privacy Program," and DoD Directive 5400.11 "DoD Privacy Program."

7.9.4 Consent to Background Checks: All Contractor and subcontractor personnel shall consent to Law Enforcement Agency Data System (LEADS) background checks. The Contractor shall conduct the background checks on all of its employees and its subcontract employees working under this contract. The Contractor and, as applicable, subcontractor shall not employ persons for work on this contract if such employee is identified as a potential threat to the health, safety, security, general well-being or operational mission of the installation and its population, nor shall the Contractor or subcontractor employ persons under this contract who have an outstanding criminal warrant as identified by LEADS through the National Crime Information Center. (LEADS checks will verify if a person is wanted by local, state, and federal agencies.) Information required to conduct a LEADS check includes: full name, driver's license number, and/or social security number, date of birth, and completion of a background check questionnaire. The Contractor shall provide this information using the Scott AFB Form 21, Contractors Consent for Background Check, and shall submit it in conjunction with the Contractor's request for either base or vehicle passes. Completion of a successful LEADS check does not invalidate the requirement for having the appropriate level of security clearance and an escort when Contractor or subcontractor personnel are working within controlled or restricted areas.

7.9.5 Proper Credentials: The Contractor shall ensure its employees and those of its subcontractors have the proper credentials allowing them to work in the United States. Persons later found to be undocumented or illegal aliens shall be remanded to the proper authorities. The Contractor shall not be entitled to any compensation for delays or expenses associated with complying with the provisions of this paragraph. Furthermore, nothing in this paragraph shall excuse the Contractor from proceeding with the contract.

7.9.6 Safety Requirements: The Contractor shall comply with the latest applicable Federal, State, Air Force, AMC, and Installation, regulations, instructions, policies, management plans and requirements regarding personnel health, occupational and operational safety (CDRL A001). The Contractor shall comply with all safety provisions, e.g., technical specifications, technical publications, and federal Occupational Safety and Health Administration (OSHA) standards (Title 29 CFR Part 1910). If there is no applicable OSHA standard, the Contractor shall use other applicable nationally or locally recognized sources of safety, health, and fire prevention standards.

7.10 CONTRACTOR PERSONNEL TRAINING

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

7.10.1 Information Assurance: Contractor shall comply with all AMC security requirements pursuant to DODI 5200.2, DOD Personnel Security Program, DODI 8500.1 Cybersecurity, and DOD 8570.01-M; Information Assurance Workforce Improvement Program. Contractor shall ensure that all personnel assigned to work on the contract shall complete Annual Information Assurance training by on-line Computer Based Training (CBT). Contractor is responsible for having the appropriate Information Assurance Level II certification coverage as defined in DOD 8570.01-M. The Contractor shall provide individual employee annual completion certificates in electronic format to the COR.

7.10.2 Antiterrorism Force Protection Level I Training: Within 30 calendar days after contract start, all contractor personnel shall complete Antiterrorism Level I Training, as required by DoDI 2000.16, DOD Antiterrorism (AT) Program Implementation: DOD Force Protection Condition (FPCON) System. Newly hired

personnel shall complete the Antiterrorism Level I Training within the first 30 calendar days of their employment. Refresher Antiterrorism Level I Training shall be completed and documented annually thereafter. The training is provided at <https://atlevel1.dtic.mil/at/> and also available through Advanced Distributed Learning Services (ADLS), Force Protection Course (ZZ133079) at https://golearn.csd.disa.mil/kc/main/kc_frame.asp for AF Portal access or <https://golearn.csd.disa.mil/kc/login/login.asp> for non-portal login.

7.10.3 Technical Currency: The Contractor shall supply and bear all training costs (e.g., salary, tuition, course materials, travel, and per diem) to ensure the technical currency of its employees on commercially available applications in order to accomplish the tasks under this contract. Some examples are operating systems, server applications, and office applications.

7.10.4 Certification Cost: The Contractor shall supply and bear all costs (salary, tuition, course materials, travel, and per diem) for its employee certifications.

7.10.5 Special Training Cost: Any special training costs resulting from changes to technology or technical direction that are related to uniquely Government applications may be reimbursed by the Government and chargeable to Other Direct Costs (ODC). Such training requires approval of the COR and the availability of the funds approval of the CO prior to registration of any training courses.

7.10.6 CSA/FSA Support Work-Center Environment Administration Support (EAS)

The contractor shall provide EAS assistance in support of the contract environments in accordance with AFMAN17-100, Air Force Information Technology (IT) Service Management, 16 Sep 2014. The EAS area of support consists of the testing, production, training, development, engineering, and prototype environments, which includes clients and servers. In order to ensure that contractor personnel have adequate permissions to provide the EAS, the contractor shall request access authorization in writing. The request shall contain an explanation of the need for the permissions, the equipment requiring the permissions, the type of permissions required, and the name of the person (s) to include his or her email address, work phone number, and evidence that the individual (s) has the requisite DOD 8570.01-M certification. The written request is to be delivered to the Contracting Officer Representative (COR) or appropriate Government agency.

8.0 TRANSITION

8.1 This paragraph addresses CDRL A001. This transition plan applies only if the contract awardee is not the same as the incumbent contract.

8.2 PHASE-IN

8.2.1 The Contractor shall provide as a management plan, a phase-in strategy and method of assuming responsibility for tasks described in the PWS and the strategy for acquiring qualified, cleared personnel. Qualified personnel include those with recent experience (last 5 years) in Oracle, UNIX, Microsoft, SQL Server, PHP, JavaScript, Visual Basic, Services Oriented Architecture (SOA), and Software as a Service (SaaS) model, along with, using a DevOps paradigm and general technical knowledge and experience with commercial cloud environments and the use of commercial cloud processes and tools. The contractor should understand and shall be capable of conforming to changing cloud and web-based technologies. Recurring status briefings shall be provided to the COR and other individuals (Other contractors and/or Government personnel) throughout the transition period. Authority: DI-MGMT-80004A.

8.2.2 Upon award, the COR and Contractor will establish contact as soon as possible. The COR will work with the Contractor to arrange, as much as practicable, a meeting(s) to process all employees facility access needs, Government CACs, and system account needs. The Contractor and COR shall conduct a joint inventory of the GFE and reconcile to the list provided in the contract as prescribed in CDRL B004. From the inventory, prepare or update the EIR (CDRL B004). Within three months after contract award, the Contractor shall have accomplished the following phase-in transition tasks:

8.2.2.1 Implement the proposed methods, processes, procedures, and tools as described in the approved transition plan

8.2.2.2 Assume Technical Support responsibilities

8.2.2.3 Assume Development responsibilities

8.2.2.4 Assume Testing and Training responsibilities

8.2.2.5 An explanation for start-up, mobilization, and transition depicting the chronological sequence of events which will be accomplished starting at contract award in order to meet all requirements of the PWS.

8.2.2.6 A listing of risks, their severity or probability and actions taken to mitigate those risks.

8.2.2.7 Within 24 hours of contract award have key staff in place in order to begin shadowing the incumbent Contractor

8.2.2.8 Immediately following the end of the phase-in period, assume full PWS services responsibilities

8.3 PHASE-OUT

8.3.1 Included in the draft Management Plan submitted to the COR six months prior to the end of the contract (CDRL A001), the Contractor shall provide a phase-out strategy describing the method of transferring responsibility for tasks described in the PWS. Recurring status briefings shall be provided to the COR and associated Contractors throughout the transition period. The Contractor shall cooperate fully with the COR and any successor Contractor(s) to ensure an orderly transition at the end of this contract (CDRL A001). The Contractor shall accomplish the following phase-out tasks:

8.3.2 Preserve and make available to the COR, if requested, copies of all records and other documentation, developed or acquired under this contract or preceding contracts for this effort, regarding performance of the work required by this contract.

8.3.3 Make available to the COR, upon request, the names, job titles, and duties of all employees who have worked under this contract.

8.3.4 Permit current employees to be interviewed for possible employment by a successor Contractor.

8.3.5 Provide an orientation for successor Contractor employees.

8.3.6 Supply to the COR, 60 days prior to the completion of the contract, the following information:

8.3.7 Complete backup of all contract and contract related data stored on each employee's hard drive, along with any global data. List of all GFE and COTS utilized in support of this task.

8.3.8 Soft and hard copies of all procedures and training materials developed as part of this effort.

8.3.9 Ensure that no contract data is corrupted, changed, or altered such that it would cause damage to the Government.

8.3.10 System documentation is to be compliant with CMMI Level 3 standards. The method of delivery will be by mutual agreement between the PMO and the Contractor.

8.3.11 Within 30 days of contract completion the Contractor shall, in conjunction with the COR, conduct a joint inventory of the GFE and reconcile to the list EIR (CDRL B004).

8.3.12 Upon contract completion the Contractor shall provide access to all information and data secured by password or key encryption card. All data locked by key card shall be unlocked prior to the turn-in or destruction of the card.

8.3.13 The Contractor shall unlock, or provide the keys to any and all equipment physically locked.

8.4 SECTION 508 ACCESSIBILITY STANDARDS / SECTION 508 OF THE REHABILITATION ACT

8.4.1 The following Section 508 Accessibility Standard(s) (Technical Standards and Functional Performance Criteria) are applicable (if box is checked) to this acquisition.

8.4.2 Technical Standards

- ☒ 1194.21 - Software Applications and Operating Systems
- ☒ 1194.22 - Web Based Intranet and Internet Information and Applications
- ☐ 1194.23 - Telecommunications Products
- ☐ 1194.24 - Video and Multimedia Products
- ☒ 1194.25 - Self-Contained, Closed Products
- ☐ 1194.26 - Desktop and Portable Computers
- ☒ 1194.41 - Information, Documentation and Support

8.4.3 The Technical Standards above assures that the maximum technical standards are provided to the Awardee. Functional Performance Criteria is the minimally acceptable standards to ensure Section 508 compliance. This block is checked to ensure that the minimally acceptable electronic and information technology (E&IT) products are proposed.

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

8.5 FUNCTIONAL PERFORMANCE CRITERIA

- ☒ 1194.31 - Functional Performance Criteria

8.6 PROTECTING GOVERNMENT INTELLECTUAL PROPERTY

8.6.1 At the completion of the contract or when turning-in Government IT resources to the COR, the Contractor shall not remove, add to, change, or manipulate data, files, computer code, operating systems, and other information residing on any Government owned/provided storage media in the use and care of the Contractor without the expressed written authorization by the CO or the COR. This requirement is invoked whether the computer files are placed there by Contractor employees in the course of Contractor performance, or otherwise provided by the Government or the Contractor. Also, in no case shall the Contractor use any method to destroy or remove data on a Government owned storage media to a point that it is not easily recoverable using OS data recovery tools, without expressed written permission of the COR. Failure of the Contractor to comply with this clause may subject the Contractor to breach of contract, criminal civil penalties, criminal charges, or all three.

8.6.2 Upon delivery of the final version release or other deliverables under this contract, and as part of contract phase-out, the Contractor shall deliver to the Government, and/or upon at the direction of the COR to transfer to another Contractor, the following:

8.6.2.1 All framework, source code (fully compliable package), libraries, database tables, scripts, resources, modules, and all other related materials on the GDSS system and all software code.

8.6.2.2 All procedures to move modules to test/production environments, maintenance procedures, reference materials, technical documentation, user manuals, training and/or classroom materials, and all other related documentation. This includes documents delivered under contract and/or documents prepared during contract performance for use under the contract.

8.6.2.3 Technical orientation of GDSS system to include definition and description of all modules.

8.6.2.4 Source code, object code, database applications, and permissions to access the source, object code, and Sybase database.

8.6.2.5 All Government furnished hardware – servers, PCs, laptops, monitors, external hard drives, cabling, switches, routers, and all peripheral devices.

8.6.3 Documentation to include system architecture documentation, configuration management procedures, (to include creating new modules, logging out existing modules, modifying code, testing, checking in modules, production releases, and version control), system administrator procedures, database structure documentation, data dictionary, and batch job schedules.

8.6.3.1 System documentation is to be compliant with CMMI Level 3 standards. The method of delivery will be by mutual agreement between the PMO and the Contractor.

APPENDIX A1 - Acronyms

ACRONYM	DEFINITION
ADIG	Architecture Data Integration Group
ADPE	Automated Data Processing Equipment
AFI	Air Force Instruction
AFNETOPS	Air Force Network Operations
AIM	Asset Inventory Management
AIS	Automated Information Systems
AISS	Applications Infrastructure and Systems Support
AMC	Air Mobility Command
AMCAT	AMC Architecture Tool
ATC	Air Traffic Control
AtC	Authority to Connect
AtC	Authority to Operate
BCR	Baseline Change Request
C2	Command and Control
CDRL	Contract Deliverable Requirements List
CFR	Code of Federal Regulations
CLIN	Contract Line Item Number
CM	Configuration Management
CMMI	Capability Maturity Model-Integrated
CMP	Configuration Management Plan
CoN	Certificate of Networthiness
COR	Contracting Officer's Representative
COTS	Commercial Off-the-Shelf
CPARS	Contractor Performance Assessment Reporting System
CPSR	Contract and Program Status Review
CPR	Contract Performance Report
CR	Change Request
DCR	Document Change Request
DID	Data Item Description
DISN	Defense and Information Systems Network
DISR	Defense Information Technology Registry
DoD or DOD	Department of Defense
DoDD	DoD Document or Doctrine
DoDI	DoD Instruction
DPO	Distribution Process Owner
DTS	Defense Transportation System
EIR	Equipment Inventory Records
EMC	Exercise Management Console
EVM	Earned Value Management
FCA/PCA	Functional Configuration Audit/Physical Configuration Audit
FOUO	For Official Use Only
FTR	Federal Travel Regulations
GDSS	Global Decision Support System
GFE	Government Furnished Equipment

GFP	Government Furnished Property
Govt/govt	Government
HQ	Headquarters
IAVA	Information Assurance Vulnerability Alert
IDD	Interface Design Description
IEEE	Institute of Electrical and Electronic Engineers
ILSP	Integrated Logistics Support Plan
ISO	International Organization for Standardization
ISP	Information Support Plan
ITAM	Information Technology Asset Management
JTR	Joint Travel Regulation
LDM	Logical Data Model
LEADS	Law Enforcement Agency Data System
MAF	Mobility Air Forces
NC	Net-Centric
NCES	Net-Centric Enterprise Services
NOTAM	Notice to Airmen
NTO	Network Tasking Orders
O&M	Operations and Maintenance
ODC	Other Direct Costs
OSHA	Occupational Safety and Health Administration
PMO	Program Management Office
PWS	Performance Work Statement
QAP	Quality Assurance Program
ROM	Rough Order of Magnitude
RSA	Requirements Specification Agreement
SDDC	Surface Deployment and Distribution Command (Army)
SEI	Software Engineering Institute
SPR	Software Problem Report
STD	Software Test Description
STR	Software Test Report
TCSD	Training Conduct Support Document
TL	Training Lesson
TRDM	United States Transportation Command Reference Data Management
TWG	Technical Working Group
USAF	United States Air Force
USCYBERCOM	United States Cyber Command
USTRANSCOM	United States Transportation Command
WBS	Work Breakdown Structure

APPENDIX A2 - Definitions

Acquisition Category (ACAT). Categories established to facilitate decentralized decision-making and execution, and compliance with statutorily imposed requirements. The categories determine the level of review, decision authority, and applicable procedures. Reference (d) provides the specific definition for each acquisition category (ACAT I through III).

Approval. To give formal or official sanction. The formal or official sanction of the activity described.

Architectures. The structure of components, their relationships, and the principles and guidelines governing their design and evolution over time.

Assessment (Assess). The act or result of determining the contribution or disposition of an activity, product, or condition, based on an appraisal of the state of IT and NSS interoperability.

Awardee: The Contractor / corporation selected for the follow-on contract.

CAF. The 'combat air forces'; the combined U.S. Active and ANG forces of bombers and fighters as well as the supporting personnel assigned to CAF.

Capability. The ability to execute a specified course of action defined by an operational user and expressed in broad operational terms. It includes the DOTMLPF required to achieve a specified course of action. It is documented in an ICD or a DOTMLPF change recommendation. In the case of materiel proposals, the definition progressively evolves to DOTMLPF performance attributes specified in the CDD and the CPD.

Certification (Certify). A formal statement of adequacy provided by a responsible Agency attesting that a system has met its interoperability and supportability needs.

Common Operating Environment (COE). Integrated software infrastructure that facilitates the migration and implementation of functional mission applications and integrated databases across information systems. The COE provides architecture principles, guidelines, and methodologies that assist in the development of mission application software by capitalizing on a thorough, cohesive set of infrastructure support services.

Conformance Testing. Testing the extent to which a system or subsystem adheres to or implements a standard.

Decision Superiority. The state at which better decisions are arrived at and implemented faster than an opponent can react, or in a non-combat situation, at a tempo that allows the force to shape the situation or react to changes and accomplish its mission.

DOD Information Technology Standards Registry (DISR). The DISR provides the minimal set of rules governing the arrangement, interaction, and interdependence of system parts or elements, whose purpose is to ensure that a conformant system satisfies a specified set of requirements. It defines the service areas, interfaces, standards (DISR elements), and standards profiles applicable to all DOD systems. Use of the DISR is mandated for the development and acquisition of new or modified fielded IT and NSS systems throughout the Department of Defense. The DISR replaced the Joint Technical Architecture.

Evaluation (Evaluate). Measuring or quantifying the value, characteristics, or capabilities of something against established standards, (as in "Test and Evaluation"). The determination of, or act of determining the relative degree to which IT and NSS interoperability is achieved.

Flight Plan. The manual or (routinely) computerized detailed plan for each segment of a flight, designed for the specific aircraft flown based on actual aircraft configuration, payload, fuel on board and winds. A flight plan details the route and the fuel remaining throughout all phases of flight.

Incumbent: The existing Contractor / corporation, operating under the existing GDSS contract.

Information Assurance (IA). Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

Information Support Plan (ISP). The identification and documentation of information needs, infrastructure support, IT and NSS interface requirements and dependencies focusing on net-centric, interoperability, supportability and sufficiency concerns.

Integrated Architecture. An architecture consisting of multiple views or perspectives (operational view, systems view, and technical standards view) facilitating integration and promoting interoperability across capabilities and among related integrated architectures.

- The operational view is a description of the tasks and activities, operational elements, and information exchanges required to accomplish DOD missions.
- The systems view is a description, including graphics, of systems and interconnections providing for, or supporting, DOD functions.
- The TV is the minimal set of rules governing the arrangement, interaction, and interdependence of system parts or elements, whose purpose is to ensure that a conformant system satisfies a specified set of requirements.

Interoperability. Interoperability is the ability of systems, units or forces to provide data, information, materiel, and services to and accept the same from other systems, units, or forces and to use the data, information, materiel and services so exchanged to enable them to operate effectively together. IT and NSS interoperability includes both the technical exchange of information and the end-to-end operational effectiveness of that exchange of information as required for mission accomplishment. Interoperability is more than just information exchange. It includes systems, processes, procedures, organizations, and missions over the life cycle and must be balanced with information assurance.

Interoperability and Supportability Needs. A condition, situation, or capability in which interoperability and supportability deficiencies have been identified, based on an approved or established rule set, test, or measure of value for judging interoperability and supportability sufficiency of IT and NSS.

Key Performance Parameters (KPPs). Those minimum attributes or characteristics considered most essential for an effective military capability. KPPs are validated by the Chairman of the Joint Chiefs of Staff.

MAF. The Mobility Air Forces are the combination of all forces supporting the MAF mission; airlifter and tanker (aircraft and crew); ground forces, assigned to U.S. Active, Reserve, and ANG units. This includes forces of other services when in direct support of the MAF.

Mission Plan. The planning of all aspects of MAF missions, by individual sortie or from point of origin to final landing. This usually includes selecting routes and reserving airspace, reserving ramp space at interim locations, acquiring Diplomatic Clearances (DIPs) for overflight and landing, etc.

Mission Critical Information System (MCIS). A system meeting the definitions of "information system" and "national security system" in reference (d) that the loss of which would cause the warfighter operations or direct mission support of warfighter operations to cease. The designation of mission critical should be made by the Head of a DOD Component, a Combatant Commander or one of their designees. MCIS is defined the same as a Mission Critical IT System.

Mission Need. A deficiency in current capabilities or an opportunity to provide new capabilities (or enhance fielded capabilities) through the use of new technologies. Mission needs are expressed in broad operational terms by the DOD Components.

Mission Plan. The planning of all aspects of MAF missions, by individual sortie or from point of origin to final landing. This usually includes selecting routes and reserving airspace, reserving ramp space at interim locations, acquiring Diplomatic Clearances (DIPs) for overflight and landing, etc.

Net-Ready. The continuous ability to interface and interoperate achieving operationally secure exchanges of information in conformance with enterprise constraints. The NR-KPP assesses the net-ready attributes required for both the technical exchange of information and the end-to-end operational effectiveness of that exchange.

Net-Ready Key Performance Parameter (NR-KPP). The NR-KPP assesses information needs, information timeliness, information assurance, and net-ready attributes required for both the technical exchange of information and the end-to-end operational effectiveness of that exchange. The NR-KPP consists of verifiable performance measures and associated metrics required to evaluate the timely, accurate, and complete exchange and use of information to satisfy information needs for a given capability. The NR-KPP is comprised of the following elements:

- Compliance with the NCOW RM.
- Compliance with applicable GIG KIPs.
- Verification of compliance with DOD information assurance requirements.
- Supporting integrated architecture products required to assess information exchange and use for a given capability.

Non-Materiel Solution. Changes in doctrine, organization, training, leadership and education, personnel or facilities that satisfy identified capability gaps.

Supportability. The ability of systems and infrastructure components, external to a specific IT or NSS, to aid, protect, complement, or sustain the design, development, testing, training, or operations of the IT or NSS to achieve its required operational and functional capability(ies).

Test and Evaluation. The act of generating data during the research and development of emerging systems and the creation of information through analysis that is useful to technical personnel and decision-makers for reducing design and acquisition risks. The process that gauges progress by measuring systems against requirements and specifications and analyzing the results.

Validation. An authoritative act or process of supporting or corroborating whether IT and NSS interoperability and supportability needs are appropriate.

Verification. The act of establishing whether IT and NSS interoperability needs are accurate, measurable, supportable, and adequately reflected for a given capability, acquisition strategy, test and evaluation plan, or in non-materiel or non-traditional acquisition IT and NSS ISPs.

APPENDIX A3 - References and Applicable Regulations

Specifications and Standards – The Government shall also provide the Contractor with access to DOD, United States Air Force, Defense Information Systems Agency, and 375th Communications Support Squadron (375th CSPTS) (or its successor organization) publications, directives, and policy letters, and any changes to this information as they are received. Contractor shall comply with the following regulations, as appropriate, within the conduct of day-to-day operations.

References/Bid Library

- AFDD 3-17 Air Mobility Operations, Chg 1, 28 July 2011
- AFI 10-701 Operations Security (OPSEC), 8 June 2011
- AFI 10-206, Operational Reporting, 21 July 2016
- AFI 10-601, Operational Capability Requirements Development, 6 November 2013
- AFI 23-111, Management of Government Property in Possession of the Air Force, 26 September 2016
- AFI 31-401, Information Security Program Management, 1 November 2005, Change 1, 19 August 2009
- AFMAN17-1203, Information Technology (IT) Asset Management (ITAM), 19 Mar 2014, Change 2, 7 March 2017
- Air Force Information Technology (IT) Service Management, 16 Sep 2014
- AFI 33-364 Records Disposition-Procedures and Responsibilities, 22 December 2006, Change 1, 6 November 2014, Certified Current 9 April 2015
- AFDPD17-1, Information Dominance Governance and Management and AFDPD 17-2 Cyberspace Operations, 12 April 2016
- AMC INFOCON Guide
- AMCI 33-105, Enterprise Configuration Management, 15 October 2000
- ANSI/ISO/ASQ Q9000: Quality Management Standards
- EIA 649 Revision B, National Consensus Standard for Configuration Management, 1 April 2011
- EIA 632, Processes for Engineering a System, 7 January 1999
- CJCSI 6212.01D, Interoperability and Supportability of Information Technology and national Security Systems, 8 March 2006.
- Combat Information Transport System (CITS)
- JP3-30, Command and Control for Joint Air Operations, 12 January 2010
- Command and Control Joint Integrating Concept 1 September 2005
- Defense Acquisition Guidebook
- Defense Intelligence Assessment: Foreign Computer Network Operations Threats to the SIPRNet, DI-2711-17-03 (July 2003)
- DOD Directive 5000.02, Operation of the Defense Acquisition System, Identified 7 January 2017, Change 2 2 February 2017
- DODI 8500.01 Cybersecurity, 14 March 2014
- DODI 8510.01 Risk Management Framework for DOD Information Technology, 12 Mar 14, Change 1, 24 May 2016
- DOD Directive 8320.1-M, Data Administration Procedures, 26 September 1991
- DOD Architecture Framework (DODAF), Version 2.02, March 2011
- DODD 0-5100.30, Department of Defense (DOD) Command and Control (C2), 5 January 2006
- DODDODI 4630.8, Procedures for Interoperability and Supportability of Information Technology and National Security Systems (NSS), 30 June 2004
- DODI 8500.2, Information Assurance (IA) Implementation, 6 February 2003
- DODI 8510.01 DOD Information Assurance Certification and Accreditation Process, 28 November 2007
- DODI 8510.01, DOD Information Assurance Certification and Accreditation Process (DIACAP), 28 November 28 2007

- DODI 8520.02 Public Key Infrastructure (PKI) and Public Key (PK) Enabling, 24 May 11
- DOD 8570.01-M Information Assurance Workforce Improvement Program, 19 Dec 05, Change 4, 10 November 2015
- (FIPS) 140-2, Federal Information Processing Standard
- GDSS Concept of Operations V1.0, 25 October 2004
- GDSS Concept of Operations V1.0, Annex 1, Deployed C2 Operations (In Coordination)
- Global Decision Support System ORD, AMC 003-81A, 20 July 01
- Global Mobility Concept of Operations (CONOPS)
- HOI 33-1, AMC Architecture Development Process
- http://www.c3i.osd.mil/org/i3/AWG_Digital_Library
- IEEE Standard for Software Maintenance IEEE 1219-1998
- IO Capstone Threat Assessment (CTA), DI-1577-31-05 (March 2005)
- ISO/IEC 12207:2008, Systems and software engineering - Software life cycle processes, 2013
- ISO/IEC 26514:2008, Systems and software engineering – Requirements for designers and developers of user documentation
- Joint C2 Functional Concept, February 2004
- Joint Deployment & Distribution Enterprise
- Joint Operations 3-0
- JP 3-30, Command and Control for Joint Air Operations, 12 January 2010
- JROCM 202-02, Global Information Grid Mission Area Initial Capability Document (GIG MA ICD) , 22 November 2002
- MAF C2 CDD: Capability Development Document (CDD) for Mobility Air Forces (MAF) Command and Control (C2) Framework dated 15 March 2006 (MAF C2 CDD).
- MAF C2 Operational Capabilities Document, dated 1 December 03
- MIL-HDBK-61a, Configuration Management Guidance, 7 February 2001
- Mobility Air Force (MAF) Command and Control (C2) CDD, 15 March 2006
- Net-Centric Environment Joint Functional Concept, 7 April 2005
- Net-Centric Operational Environment Joint Integrating Concept, 31 October 2005
- Net-Centric Operational Environment Joint Integrating Concept, 31 October 2005
- NII/DOD CIO Net Centric Checklist
- ORD AMC003-81A
- USTRANSCOM 2011 Strategic Vision
- DoDI 2000.16, DOD Antiterrorism (AT) Program Implementation: DOD Force Protection Condition (FPCON) System.

ATTACHMENT 1 – Sample: What's New Document

- Sample 'New Document' for a GDSS Release. This document shall present all new features in a release, with a brief plain English overview of the new feature, and states the procedure on how it works. All fixes that effect any change in how the user operates the software will also be identified, with an explanation of how it changes the utility (i.e. work-arounds replaced).
- GDSS Version 3.0.1. The software corrections allocated to this version address problems where GDSS does not fully satisfy the stated system requirements. The new features allocated to this version addresses new system features and capabilities, including views of the new mission visualizing tool, conversion of some features to Web Applications, and new crew scheduling functionality. This document provides a general description of each of the BCRs. The BCRs described in this document are listed in groupings by application.

New Mission Planner Feature	
	This new feature provides the user with a graphic tool to be able to display the mission as an overlay on Google Earth ©. This is an option for power users; flight planners, Flight Managers, and Dip Clearance Officers to view a flight safety level picture of the mission route, capture way points, country IFR boundaries, etc. Users will be required to have Google Earth © installed on their workstations. To use this feature, a simple right click and selection of the GE will pivot them to GE and see the mission selected in a new window.
Web Login	
	This release provides an automatic password reset process for GDSS users. If CAC based password generation utilities are available on the system, the user may perform self-initiated password reset through use of their CAC and CAC related PIN.
New Crew Scheduling Capabilities	

New Mission Planner Feature	
	Individual Crew Readiness can now be associated with category of crew required. It is a default setting to filter out crewmembers that are not eligible to fly based on business rules. It can be deselected at the discretion of the user.

DRAFT

ATTACHMENT 2 – Non-Disclosure Agreement

Non-Disclosure Agreement for Contractor Employees Supporting AMC Contracts

NOTE: This Non-Disclosure Agreement is an agreement designed for use by Contractor (including subcontractor) employees assigned to work on AMC contracts. Its use is designed to protect non-public Government information from disclosure and prevent violations of federal statutes/regulations. The restrictions contained in this agreement also serve Contractors by promoting compliant behavior that keeps Contractors eligible to compete for Government contracts. In addition to the potential impact on future business opportunities, failure to abide by this agreement could result in administrative, civil or criminal penalties specified by statute or regulation.

"Non-public information," as used herein, includes trade secrets, confidential or proprietary business information (as defined for Government employees in 18 USC 1905); advance procurement information (future requirements, acquisition strategies, statements of work, budget/program/planning data, etc.); source selection information (proposal rankings, source selection plans, Contractor bid or proposal information); information protected by the Privacy Act (social security numbers, home addresses, etc.); sensitive information protected from release under the Freedom of Information Act (pre-decisional deliberations, litigation materials, privileged material, etc.); and information that has not been released to the general public and has not been authorized for such release (as defined for Government employees in 5 CFR 2635.703).

1. I, _____ currently an employee of _____, hereby agree to the terms and conditions set forth below:
2. I understand that I will have access to confidential business information (as defined by 18 USC 1905), Contractor bid or proposal information (as defined by FAR 3.104-3), and/or source selection sensitive information (as defined by FAR 3.104-3) either for contract performance or as a result of working in a AMC facility or of working near AMC personnel, Contractors, visitors, etc. I fully understand that such information is sensitive and shall be protected in accordance with 41 U.S. Code Section 423 and 18 U.S. Code Section 1905 and FAR Part 3. I also certify that I do not have any real or apparent conflicts of interest with respect to the information disclosed. If any potential conflicts of interest, real or otherwise, do present themselves, then I shall immediately disclose the pertinent information that may be a potential conflict to an agency ethics official who shall review the circumstances.
3. In the course of performing under contract/order number _____ or some other contract or subcontract for the AMC I agree to:

- a) Use only for Government purpose any and all confidential business information, Contractor bid or proposal information, and/or source selection sensitive information to which I am given access. I agree not to disclose "nonpublic information" by any means (in whole or in part, alone or in combination with other information, directly or indirectly or derivatively) to any person except to a U.S. Government official with a need to know or to a non-Government person (including, but not limited to, a person in my company, affiliated companies, subcontractors, etc.) who has a need to know related to the immediate contract/order, has executed a valid form of this non-disclosure agreement, and receives prior clearance by the contracting officer. All distribution of the documents will be controlled with the concurrence of the contracting officer.
 - b) Not use such information for any non-Governmental purposes, including, but not limited to, the preparation of bids or proposals, or the development or execution of other business or commercial ventures.
 - c) Store the information in such a manner as to prevent inadvertent disclosure or releases to individuals who has not been authorized access to it.
4. I understand that I shall never make an unauthorized disclosure or use of confidential business information, Contractor bid or proposal information, and/or source selection sensitive information unless:
- a) The information has otherwise been made available without restriction to the Government, to a competing Contractor, or to the public;
 - b) The contracting officer determines that such information is not subject to protection from release.
5. I agree that I shall not seek access to "non-public information" beyond what is required for the performance of the services I am contracted to perform. I agree that when I seek access to such information or attend meetings or communicate with other parties about such information, I will identify myself as a Contractor. Should I become aware of any improper or unintentional release or disclosure of "non-public information," I will immediately report it to the contracting officer in writing. I agree that I will return all forms (including copies or reproduction of original documents) of any "non-public information" provided to me by the Government for use in performing my duties to the control of the Government when my duties no longer require this information. By signing below, I certify that I have read and understand the terms of this Non-Disclosure Agreement and voluntarily agree to be bound by its terms.

Signature of Employee/ Date

Printed Employee Name

Signature of Company Official/ Date

Printed Company Official Name

DRAFT

ATTACHMENT 3 – Sample SPR and BCR

- 7.6.3.1.1 SPRs and BCRs will all have the following features for control purposes:
- 7.6.3.1.2 IDENTIFICATION. Control number, date submitted, system identification (title, version, and environment), point of contact (name, office, contact information).
- 7.6.3.1.3 DESCRIPTION. (See example below) Short title, description of change, source documentation; severity, classification, priority; justification, functional impact, workaround, attachments.
- 7.6.3.1.4 ANALYSIS. Cost estimates by functional analyst, data system analyst, developer; program analysis, name of analyst, recommended action; targeted release version.
- 7.6.3.1.5 APPROVAL. Functional manager comments; checks for requirements manager, configuration management, test manager.
- 7.6.3.1.6 ACTION. Disposition, date completed; delivered, accepted, date closed.

SPRs and BCRs (CRs) are NOT requirements. They all must go through a disciplined process that refines the CR; in the case of SPRs, they shall provide the expected behavior and the problem noted, the requirement in terms of ‘what needs to be fixed’, and the testable outcome. It does not include a solution (although a solution may be expressed as an example of a desired outcome). It does not include the test steps; rather it states what the outcome of the test will be.

Item 1	GDSS, Thick Thin Discrepancy on Tail #
SPR	Expected Behavior: List of available missions within time selected should be presented. On the web, the Schedule Mission display did not display the list of available missions (GO button) if: - The selected tail # already has a mission scheduled - The current time is later than the first departure time. Created mission ABB01NOSP235 and scheduled tail # 70043 - Opened Aircraft Summary on web and noted that the above mission was assigned to tail # 70043 - At a time before the first ETD, right clicked on tail # field and clicked GO button on Schedule Mission display. Noted that list of available mission is presented at the bottom of the form. Confirmed same functionality on thick client - Waited until after initial ETD, right clicked on tail # field and clicked GO button on Schedule Mission display. Problem: Noted the list of available missions is not presented at the bottom of the form. Confirmed that the list is presented on thick client. On web, the user is able to manually enter mission number in the applicable field and complete the scheduling process. The missions that should be displayed in the mission search grid of the web are not being displayed correctly. Requirements

	R1: The Schedule Mission display shall display all missions that meet the Mission Search Criteria. R1.1: Missions displayed shall not exceed the user Roles/Privileges. Testable Outcomes T1: The Schedule Mission display displays all missions that meet the Mission Search criteria. T1.1: Missions shall be returned when the list is evoked from an aircraft assigned to a mission that has an initial departure before the current time. T1.2: Special Access missions are not returned unless the user has the proper Roles/Privileges to see Special Access missions.
Item 2 BCR	Add Dip Route Field to Country Record Current Behavior: There is no field in the Dips app for "route of flight". What is needed to accommodate a huge time savings is a data field to the diplomatic worksheet, country record for dips "route of flight." The new data element shall be required to accommodate a manually entered 200 ASCII character text string. Also; 1) This field is not printed on the mission detail. Data element may be left blank. 2) This data element shall be retrievable via SQL query or in a future GDSS-MEIS-APACS interface. 3) Optional req: this data element shall be added to the dips summary country view as a customizable column. Needed for v3.0.0 release. Requirements: R1: Add a data field to the DIP Worksheet country record for dips "route of flight" that shall accommodate 200 ASCII characters R2: This field is not printed on the mission detail R3: This field is optional. R4: This data element shall be retrievable via SQL query R5: This data element shall be retrievable in a future GDSS/MEIS/APACS interface R6: OPTIONAL: Add this field to the DIP Summary Country View as a customizable option Testable Outcomes: T1: Verify there is a Route of Flight data field on the DIP Worksheet country record T2: Verify this field is not printed on the mission detail T3: Verify this field is optional T4: Verify this field is retrievable via a SQL query T5: Probably can't do the GDSS/MEIS/APACS interface part