PERFORMANCE WORK STATEMENT (PWS)

Global Decision Support System (GDSS)
Application, Implementation, Modernization, and Support (AIMS)

8 May 2024

Contents

1. BACKGROUND

GDSS is an extension of the USTRANSCOM network providing a full computing infrastructure to include network, servers, security, and storage. Replication is provided using two near real-time replicated unclassified and classified C2 enclaves for redundancy and performance. Currently, there are 21,000 active user accounts from 261 major sites world-wide. GDSS user demographics include aerial port, aircrew (flying and medical), airfield managers, C2 controllers, diplomatic clearance, flight managers, flight planners, intelligence, maintenance, mission planners, stage managers, transportation managers, and weather. GDSS interfaces with over twenty systems in both the unclassified and classified domains.

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. The COTS products supporting the current design include Oracle and Microsoft products.

GDSS is deployed on the USTRANSCOM Distributed Enclave (DE) in a multi-master replicated fail-over environment on host infrastructures maintained by the Government. General DE network operations and maintenance is directed by the Government, to include local network updates/patches as part of their security policies. GDSS Object Processor (GOP)/Mobility Enterprise Information Service 3 (MEIS 3) and GDSS Object Processor (MGOP) is planned for sundown; required services and components are being migrated to GDSS DB as directed by the Government. Support will continue for these components until sundown is complete.

The GDSS Mobility Communication Services (MCS) component is utilized to communicate with external interface partners e.g., MEIS 4, Consolidated Air Mobility Planning Systems (CAMPS), Mobility Air Forces Automated Flight Planning Services (MAFPS). MCS reads and writes data to several MEIS 4 services and provides monitoring of these services on both the unclassified and classified domain to ensure the data remains in sync with external interface partners. The GDSS Cross Domain Service (CDS) sends required GDSS data low-to-high (L2H) utilizing a cross domain filter residing within the DISA Cross Domain service. A high-to-low (H2L) CDS data flow is under development. The CDS component services require monitoring to ensure data remains in sync between unclassified and classified GDSS domains.

Additionally, USTRANSCOM has directed the migration of GDSS to a Cloud environment. GDSS anticipates being fully migrated into the unclassified and classified Cloud One environments during this contract. After migration to the Cloud environments, GDSS will still maintain a small portion of its On-Prem systems, for example Mobile Service Devices on the CENTCOM Regional Intelligence Exchange System (CENTRIX) domains.

Example technologies for maintaining GDSS include, but are not limited to: Oracle, JavaScript, Visual Basic, .Net, Java, Microsoft Windows Server, Microsoft Windows Active Directory, ActivClient, Visual Basic Vbscript, Visual C++, Internet Information Services, Microsoft SQL Server, Nessus, PHP, ActiveState ActiveTcl Enterprise, WinZip, ArcGIS Server, McAfee Endpoint Security, Denodo, Simple Mail Transfer Protocol, Internet Protocol version 4 and 6, Extensible Markup Language (XML), Load balancers, Transport Layer Security (TLS), Amazon Web Services, etc.

2. Purpose and Scope

This effort is to provide Application, Implementation, Modernization, Support (AIMS) and sustainment of the Global Decision Support System (GDSS) program. Application support and sustainment must take into consideration and incorporate older and modern technology. Most recently, new requirements have established a need for a more global capability supporting disconnected operations and data sharing. These requirements must support existing operations while transitioning to the global capability.

Program activities for GDSS are managed by the Headquarters Air Force Lifecycle Management Center (AFLCMC)-Operating Location–2 (OL-2 /HBMSA, GDSS Program Management Office (PMO)). Responsibilities of this office include managing funds, schedule, software sustainment and implementation, software operations and maintenance, and hardware acquisition for the GDSS software applications. The scope of effort for this requirement is to sustain, develop, modernize, deliver, test, field, and maintain applications within an Agile/DevSecOps software construction methodology supporting designated Mobility Air Forces (MAF) portfolio of applications. Services and products being procured are referred to as Agile Application Development in total. Services will be provided in the form of technical and support tasks associated with Mobility Air Forces Command and Control (MAF C2) projects, programs, applications, and infrastructure. The goal is to utilize, to the greatest extent possible, Agile/DevSecOps sustainment, development best practices, guidelines and parameters. Development and maintenance includes applications within the United States Transportation Command (USTRANSCOM) and Air Mobility Command (AMC) IT enterprise, to include Cloud based (ref 1.2.5.3 and 1.2.5.4.) and On-Premises classified and unclassified environments.

The scope of this PWS is to provide the following for GDSS:

- Provide application software sustainment
- Provide operational application management
- Provide transition support
- Provide functional support
- Provide modernization support

3. Performance Requirements

3.1 Task Area 1 - Program Management

3.1.1 The Contractor shall establish and provide a qualified workforce capable of performing the required tasks. The workforce shall include a program manager who will oversee all aspects of the contract. The Contractor shall maintain 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. All deliverables shall meet professional standards for technical writing and the requirements set forth in the contract and shall clearly identify assumptions.

3.1.2 The Contractor shall identify and 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 tracked, and lessons learned incorporated into applicable processes. The contractor shall establish and maintain a documented set of disciplined, mature, and continuously improving processes for administering all contract efforts with an emphasis on cost-efficiency, schedule, performance, responsiveness, and consistent, high-quality delivery.

3.1.3 The contractor shall provide a Technical and Management Work Plan (A001) to meet stated Government requirements and must advise the COR as soon as possible whenever requirements cannot be met. Actual or projected failure to meet PWS requirements shall be reported to the COR as soon as the information is available and in the appropriate periodic reports, test reports, and review minutes.

3.1.4 **Subtask 1-4 – Meetings**

The Contractor shall support and participate in meetings as requested by the Government. The Contractor shall generate presentation materials in order to aid in the discussion of technical issues and will support conferences, meetings, demonstrations, and Technical Interchange Meetings/Reviews. The Contractor shall also provide agendas, meeting minutes, and track

action items associated with the aforementioned meetings/reviews (CDRL A004). The Contractor shall not conduct any external meetings, conferences, or presentations, whether planned or ad hoc, with other Government organizations other than the PMO or outside agencies, to discuss any program requirements, policies, etc., without first obtaining the permission of the COR.

3.1.4.1 The Contractor shall conduct and provide, during the meeting, a presentation providing a detailed overview of the GDSS contract progress. The briefing shall include, at a minimum, the reportable items listed below plus any additional items directed or agreed to by the Contractor and COR.

3.1.4.1.1 Schedule and Progress, which includes:
a. Milestone Dates (projected vs. actual)
b. Problem Reports Reported/Resolved
c. Changes Implemented

3.1.4.1.2 Resource Utilization (Phase Man-hours and Cumulative Man-hours)

3.1.4.1.3 Growth and Stability, which includes:
a. Requirements (status/progress)
b. Functional Support (Customer Problems/Resolution, Software Issues, etc.)

3.1.4.1.4 Product Quality (Performance, Serviceability, Durability, Usability to meet government expectations)

3.1.4.1.5 Problem Report Trends of hours worked resulting from correcting defects discovered during testing, fielding, and within 30 calendar days after fielding. The trend will include comparison, analysis, and action taken to reduce hours resulting in defect correction work. The timeline will include previous releases/fielding's up to the latest activities.

3.1.4.2 The following is a non-exhaustive list of meetings that may be necessary:

- GDSS Staff Meetings
- GDSS Program Management Office & Contractor PM meeting Program Management Review
- Chief Information Office (CIO) Program Review preparation Meetings
- Ad hoc teams support (as requested by the COR)
- Accreditation and Security Support Meetings (as requested by the COR)
- Information Support Plan (ISP) Meeting support (as architecture changes or software releases dictate)
- Technical Working Group (TWG) Meeting support (as requested by the COR)
- Process Improvement Management Meetings (as requested by the COR)
- USTRANSCOM and AMC Sponsored Meetings (as requested by the COR)

3.1.5 **Subtask 1-6 - Task Progress**

The Contractor shall provide Visibility/Monitoring of Task Progress by accomplishing the following:

3.1.5.1 Provide Contractor's Progress, Status, and Management Reports (CDRL A002) summarizing the monthly efforts under the contract for each task and subtask.

3.1.5.2 Provide an Integrated Program Management Report (IPMR) (CDRL A005) to include:

a. Establish, integrate, and report the program-wide Work Breakdown Structure (WBS) up to Level 3, align with the tasks described in this PWS, and as described in MIL-HDBK-881, Department of Defense Handbook Work Breakdown Structure, which may be further defined or modified by the Program.

b. Maintain and annotate an Integrated Master Schedule (IMS) of all Contractor activities associated with the efforts described in tasks 1 through 5 utilizing the tools identified by the COR, e.g., Microsoft Project.

i. Populate each schedule with sufficient task activities to ensure visibility of management and tracking for each milestone.

ii. Identify, within the schedule, the resources required to accomplish all task activities. Contractor may use generic resource identification.

iii. Determine and annotate appropriate milestones needed to ensure/monitor progress.

iv. Baseline all schedules with concurrence by the COR.

v. Update schedule progress on a weekly basis. Provide schedule status, risks, issues and progress.

3.1.5.3 Provide Contract Funds Status Reports (CDRL A008)

3.1.5.4 Provide Funds & Labor Hour Expenditure Reports (CDRL A003)

3.1.5.5 Provide Equipment Inventory Records IAW Section 3.11 (CDRL A007)

3.1.5.6 Brief the progress of each assigned task, address schedule tracking concerns/impacts to the master schedule, and to solicit input from the Program Manager or Contracting Officer's Representative (COR). Contractor's Technical & Management Work Plan (CDRL A001)

3.2 Task 2 - Application Software Sustainment

The Contractor shall provide software sustainment/enhancements for the current GDSS applications and capabilities based on mission-driven PM and Functional Manager priorities/coordination. The Contract shall follow the software milestone release processes are addressed in this section.

3.2.1 Subtask 2-1 - Software Release Planning

The Contractor shall provide the support necessary to maintain the GDSS software via the acceptance process described in the GDSS Configuration Management Plan (CMP). The Contractor shall provide and follow its Software Development Plan (SDP) (CDRL A011) that compliments the GDSS software release process as described in the GDSS CMP. In order to set a proper requirements baseline for each release, the Contracting Officer Representative (COR) produces a Release Specification Agreement (RSA) through its configuration control boards and Joint Version Planning Meetings (VPMs). The details for the individual requirements are maintained in the COR-approved database. The RSA forms the baseline for the release and will include the requirements and Contractor's delivery schedule for that release. Once signed, changes to or deviations from the RSA (requirements baseline) require a revised and COR-approved modification to the RSA.

3.2.2 Subtask 2-2 – Configuration Management

Due to the migration to a commercial Cloud and implementation of a DevSecOps paradigm, there may be necessary adaptive changes to configuration management processes and the Contractor shall agree to implement those processes as necessary. The Contractor shall provide the following Configuration Management activities for each release:

Using MIL HDBK 61B, ISO/IEC/IEEE 12207:2017, 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 enhancements 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 build process. Authority: DI-SESS-80858D. The Contractor shall provide a software Configuration Management Plan (CMP) (CDRL A021).

The Contractor shall accomplish the following:

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

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

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

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

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

3.2.2.6 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.

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

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

3.2.2.9 Establish and maintain records describing configuration items.

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

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

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

3.2.2.13 Ensure configuration controls 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.

3.2.2.14 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.

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

3.2.2.16 Ensure CM processes and procedures align with the Government's Configuration Management Plan (CMP).

3.2.2.17 Provide traceability and visibility to the PMO for all Change Requests (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.

3.2.2.18 Ensure CM of software 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.

3.2.2.19 Understand that the migration to a commercial Cloud environment and implementation of a DevSecOps paradigm there will be adaptive changes to configuration management processes and the Contractor shall agree to implement those processes as necessary.

3.2.2.20 Maintain the Cloud One technical and functional baselines in all environments in a government-approved code repository and artifact repository.

3.2.2.21 Provide Configuration Management (CM) for the complete lifecycle of all software deliveries (e.g., release, hotfix, warm fix, security patch, configuration change), to include installation, operations, installation instructions, and support documentation.

3.2.2.22 Update existing Cloud One Configuration Management Plan (CMP), in coordination with the GDSS PMO, documenting the processes and procedures for maintaining the functional and technical requirements and program baseline throughout all environments.

3.2.2.23 Provide reports of the GDSS Production and Non-Production baselines (CDRL B012) to include component version identifiers for each environment/suite to the Government upon request or via automated method.

3.2.3 **Subtask 2-3 - Analyze**

The Contractor shall provide analysis support by accomplishing the following tasks:

3.2.3.1 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 Contracting Officer and COR with estimate labor hours only, to work the task.

3.2.3.2 When requested, propose refinements and analysis to use cases, CRs (Baseline Change Reports (BCRs) and Software Problem Reports (SPRs)) (CRDLs 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 2 for standards for CRs.

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

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

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

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

3.2.4 **Subtask 2-4 - Design**

The Contractor shall design software to meet requirements by completing the following tasks; meeting the plans, specifications, and descriptions accepted by the COR under Task 1; and the COR-approved analysis conducted by the Contractor under Subtask 2-3 (paragraph 2.2.3):

3.2.4.1 Design and document software architecture, including incorporating business rules, data flow diagrams, algorithms, user stories, and special COTS and Government Off the Shelf (GOTS) features.

3.2.4.2 Prepare software design products in industry standard formats, modeling tools and specifications (e.g. Extensible Markup Language (XML) Schema Documents (XSDs) using tools like XMLSpy, and relational data models using tools like Erwin, Web Service Definition Language (WSDL), Simple Object Access Protocol (SOAP)) to support technical review and approval of software direction and decisions.

3.2.4.3 Conduct design reviews. Provide design artifacts to the COR not less than 1 full work day prior to the design review.

3.2.4.4 Provide an updated Database Design Description (DBDD) (CDRL A015) if the design process results in changes to the database (e.g., schema, stored procedures, index, table space allocation, constraint, etc.).

3.2.4.5 Provide an updated Installation and Operations Document (IOD) (CDRL A002) and/or Threat Model (CDRL A018) if the design process results in changes to the installation procedures or security model.

3.2.4.6 Provide sustainment and configuration management of the GDSS data model utilizing tools like Erwin.

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

3.2.4.8 Participate in the Services Working Group as requested by the COR to assist in the sustainment and configuration management of the COR-provided enterprise-level and system centric Interface Design Descriptions (CDRL A014) and Services Definition Framework.

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

3.2.4.10 Create prototypes, mock-ups, and storyboarding as required for version requirements.

3.2.4.11 Document all requirements clarifications, prototypes, mockups, storyboards under CM control and make them available for reference during internal and GDSS design reviews.

3.2.4.12 Evaluate designs and requirements to ensure GDSS security compliance is maintained. Perform threat modeling and design against modeled threats. Provide recommendations to the COR regarding best practices derived from Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs) and industry sources.

3.2.4.13 Present results of release design to the COR to obtain a go / no-go decision by the Government before moving into release coding (this can be accomplished on an iterative basis).

3.2.5 **Subtask 2-5 – Build**

This task outlines the activities to enhance on-premise environment(s) and to modernize and transition applications to Cloud One, leveraging cloud-managed services and automated pipeline technologies to the greatest extent possible. The desired end-state is to realize Continuous Integration (CI)/Continuous Delivery (CD) as part of DevSecOps for the following environments:

3.2.5.1 On-Premises classified and unclassified production environments to include NIPR and SIPR. DevSecOps will only be considered in the On-Premises environments if there is an issue preventing Cloud One migration from completing.

3.2.5.2 The Contractor shall provide the support necessary to maintain the GDSS software via the Government's sustainment and approval processes. The GDSS program utilizes Agile for on-prem environment(s) software sustainment. 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 build 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.

3.2.5.2.1 **On-Prem Major Release Frequency**

The Contractor shall deliver two or more major releases per each period of performance supporting GDSS (CDRL C009). During period of performance, the Contractor shall be responsible for any fixes from the prior major release version delivered. 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 into a single package. The number of requirements will be determined and prioritized by the Government. Within the agile development framework, multiple incremental deliveries will be rolled up to produce a single major release. Delivery dates and schedules are established 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 or more 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.

3.2.5.2.2 **On-Prem Corrections, Hot Fixes, Warm Fixes, & Patches**

The Contractor shall deliver 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. Prior to a small sustainment software delivery release, the Contractor needs to respond to operational issues and provides a solution.

3.2.5.3 **INFO: Non-Production Cloud One IL5 and IL6 Virtual Private Clouds (VPCs):**

a. Cloud One Non-Production VPCs and all systems within them.

b. Zone A VPCs – Mirror of the Production environment to the greatest extent possible; Used for software development, testing (e.g., security, functional, interoperability), and validation before pushing to Production. (e.g., MobNet, V&V)

c. Zone B VPCs – Integrated build and security scanning. No testing or external connections allowed.

d. Zone C VPCs – Software development; Only outbound connections allowed.

3.2.5.4 **INFO: Production Cloud One IL5 and IL6 VPCs:**

a. Cloud One Production VPCs and all systems within them.

b. IL5 VPCs includes Operational. (e.g., Training, Exercise, V&V)

c. IL6 VPCs include Operational. (e.g., Training, Exercise, V&V)

3.2.5.5 **Cloud Environment:**

The Contractor shall:

a. Provide Agile/DevSecOps software support for GDSS.

b. Provide the necessary Amazon Web Services (AWS) and Cloud One expertise to build, secure, deploy, and maintain GDSS, Non-Production, and Production environments in the IL-5 through IL-6 Government Cloud One environments.

c. Provide the AWS and Cloud One expertise required to operate, secure, and maintain the Development, Non-Production, and Production Cloud One environments to reliably and efficiently develop, compile, build, test, and deploy secure code and instances.

d. Provide access to all tools, repositories, and resources upon request and approval from the Government.

e. Follow, implement, and integrate the Mobility Air Forces Command and Control Family of Systems (MAF C2 FoS) Enterprise DevSecOps Process into the existing build processes between the development environment and the Cloud One Non-Production and Production environments.

f. Within 30 calendar days of task award and annually thereafter, deliver an updated Software Development Plan (SDP) to include the integration of the MAF C2 FoS Enterprise DevSecOps Process, to include a mapping from the vendor software processes to the MAF C2 FoS Enterprise DevSecOps Process activities/steps associated with the "DEV" actor.

g. Execute DevSecOps processes in accordance with Government-approved Software Build Plan and coordinate any changes to processes with the Government at least 30 calendar days prior to implementing a change.

h. Implement the following DevSecOps principles; automated build/security scanning, Infrastructure-as-Code (IaC), Configuration-as-Code (CaC), Non-Service Interruption (NSI) deployment patterns (e.g., Blue/Green, Canary deployments), monitoring, Static Application Security Testing (SAST), and Dynamic Application Security Testing (DAST).

i. Provide technical designs and recommendations for introducing cloud-native tools, services, and processes into the GDSS baseline.

j. At the direction of the Government, implement solutions to optimize GDSS using, as well as implementing, cloud-native tools and services in support of continued efficiency and operation within Government cloud environment(s).

k. Build and maintain GDSS automated pipelines to build, deploy, and test the builds/releases from the development environment to the Cloud One Production and Non-Production environments.

l. Deliver two physical copies of pipeline artifacts (e.g., GitLab exports, Artifactory exports, Jenkins jobs, source code, build scripts, executables) for each software release or as specified by GDSS Government leadership.

m. Update current GDSS Identity & Access Management (IdAM) techniques, processes, and procedures to ensure successful authentication and authorization of accounts (e.g., user, interface, application) within the Cloud One environments.

n. Build and maintain AWS Machine Images (AMIs) to create the needed AWS services in the GDSS Cloud One VPCs.

o. Recommend automated testing improvements (e.g., unit, system integration, regression, security, performance, failover, interface, interoperability) and as directed by the Government, build/deliver/implement automated tests, to verify that the software meets test pass/fail criteria for each requirement.

p. Ensure all security requirements, such as STIG and Security Requirements Guides (SRG) applicable to the programs are implemented as part of the GDSS build process, automating to the greatest extent possible as directed by the Government.

q. Ensure the DevSecOps processes provide traceability of technical and functional requirements throughout the GDSS lifecycle.

r. As directed by the government, perform all actions necessary to transfer GDSS code and artifacts between the NIPR/IL5 and SIPR/IL6 domains following government-approved transfer processes/procedures.

3.2.6 **Sub-Task 2-6 - Monitoring**

3.2.6.1 Create and deliver a Cloud One Monitoring Plan that meets the GDSS availability requirement of 99.999%, leveraging cloud-native capabilities and limiting manual monitoring of GDSS to the greatest extent possible within 45 calendar days of task award.

3.2.6.2 Implement the monitoring plan as approved by the Government within 20 calendar days of approval.

3.2.6.3 Create and provide Monitoring reports on a monthly basis that display usage metrics and trends.

3.2.6.4 Design, build and deploy monitoring tools to highlight trends and proactively identify problems that could impact system stability and system availability with Government approval when cloud-native capabilities are not feasible.

3.2.6.5 Design, build and deploy automated response scripts for specific known error/failure conditions that can be executed by the MAF C2 Enterprise Help Desk (e.g., SIAOMS) as an initial response action to system or application alerts and update System and Application Monitoring/Troubleshooting procedures for each change.

3.2.6.6 Recommend areas for implementing automated health checks and self-healing in an effort to reduce the overall downtime of the system.

3.2.6.7 Monitor the Non-Production environments during normal duty hours to ensure that the Non-Production environments are available for development and testing.

3.2.7 **Sub-Task 2-7 - Infrastructure Development and Deployment**

3.2.7.1 Request and gain Government approval prior to planning for and/or deploying new and/or modifying cloud resources/services in the designated cloud environment (e.g., Cloud One).

3.2.7.2 Manage and sustain the Cloud One AWS Workspace Virtual Desktop Infrastructure (VDI) Development environment utilized to support GDSS. For the purposes of this PWS, all references to AWS Workspace VDI include supporting components for this solution (e.g. PostgreSQL RDS, AWS Managed Active Directory (AD), Guacamole Containers, GitLab EC2).

3.2.7.3 Sustain, patch, and deploy the AWS WorkSpaces VDI via an automated pipeline process.

3.2.7.4 Monitor the AWS Workspaces daily to include resources (e.g. CPU, Storage, etc.) , vulnerabilities, etc.

3.2.7.5 Create, update, and manage user roles within Cloud One Active Directory via an automated pipeline process.

3.2.7.6 Create, update, and manage security controls/policies/directives within the AWS Workspaces via an automated pipeline process.

3.2.7.7 Create, update, delete users via an automated pipeline process or manually in AWS Managed Active Directory (AD) in accordance with GDSS account management processes.

3.2.7.8 Manage, update, and deploy tools on the AWS WorkSpaces VDI images via an automated pipeline process.

3.2.7.9 Coordinate and gain Government approval for all changes to the AWS WorkSpaces VDI images and development tools installed on them with the GDSS PMO.

3.2.7.10 Establish a configuration management process to include compliance audits for ensuring the AWS Workspace VDI baseline is maintained in accordance with GDSS accreditation and programmatic requirements.

3.2.7.11 Provide RMF support to include diagrams, scan results, etc. for the AWS Workspace VDI as required by GDSS

3.2.7.12 Build and deploy virtual machine images (e.g., Amazon Machine Images (AMI)) in the Non-Production and Production environments to support GDSS.

3.2.7.13 Ensure virtual machine images are compliant with security directives (e.g., STIG, Cyber Task Orders (CTO), Task Orders (TASKORD)).

3.2.7.14 Ensure virtual machine images do not contain Severity Category Codes (CAT) I vulnerabilities (https://public.cyber.mil).

3.2.7.15 Deploy virtual machine images via an automated delivery, pipeline process.

3.2.7.16 Leverage AWS base AMIs as much as possible.

3.2.7.17 Identify custom AMIs to the Government for approval prior to implementation in the event a custom AMI is required.

3.2.7.18 Build and deploy containers (e.g., Elastic Container Service (ECS)) in the Non-Production and Production environments to support GDSS.

3.2.7.19 Ensure containers are compliant with security directives (e.g., STIG, Cyber Task Orders (CTOs), Task Orders (TASKORD)).

3.2.7.20 Ensure containers do not contain CAT I vulnerabilities.

3.2.7.21 Deploy containers via an automated delivery, pipeline process.

3.2.7.22 Deploy and sustain virtual machines (e.g., Elastic Compute Cloud (Amazon EC2)) instances in the Non-Production and Production environments to support GDSS.

3.2.7.23 Deploy and configure virtual machines via an automated delivery, pipeline process.

3.2.7.24 Utilize and comply with the Government's naming/tagging convention for virtual machines.

3.2.7.25 Comply with all required security (e.g., STIG, SRG), financial (e.g., Financial Information System Control Audit Manual (FISCAM), and programmatic requirements for virtual machines.

3.2.7.26 Ensure that virtual machines do not contain CAT I vulnerabilities.

3.2.7.27 Manage the virtual infrastructure (e.g., Amazon VPC) in the Non-Production and Production environments to support the MAF C2 applications.

3.2.7.28 Deploy virtual infrastructure via an automated delivery, pipeline process.

3.2.7.29 Utilize and comply with the Government's naming/tagging convention for virtual infrastructure.

3.2.7.30 Build and deploy Network Access Control Lists (ACLs) and Security Groups to ensure Cloud resources (e.g., VPCs, EC2 Instances, Load Balancers) are protected from network intrusions and other malicious activities.

3.2.7.31 Deploy network ACLs and Security Groups via an automated delivery, pipeline process.

3.2.7.32 Ensure all security (e.g., STIG, SRG, TASKORD), financial (FISCAM), and programmatic requirements related to security of the instances are implemented and enforced.

3.2.7.33 Build, deploy, maintain, and use system, network and security tools and utilities (e.g., Tanium, Crowdstrike, SolarWinds) as requested and approved by the Government.

3.2.8 **Subtask 2-8 - Load Balancing, Auto Scaling, and Networking**

3.2.8.1 Design and deploy load balancing solutions that provide increased user uptime and GDSS survivability during planned/unplanned outages.

3.2.8.2 Design and deploy load balancing solutions to respond to GDSS resource monitoring tools alerts and automatically move users and interfaces to available resources.

3.2.8.3 Design and deploy system scaling solutions to ensure the applicable GDSS resources are available when an increased workload is experienced.

3.2.8.4 Manage all internal and external network connections in the Non-Production and Production environments, to include:

a. Document Network ACLs and all changes.

b. Document PPSM and all changes.

c. Provide written instructions for the MAF C2 Enterprise Help Desk (e.g., SIAOMS) to update Production network connections.

d. Coordinate network changes with Cloud Service Provider.

3.2.9 **Sub-Task 2-9 - Cloud Issue Escalation**

3.2.9.1 Submit Jira tickets to the Cloud Service Provider (CSP) (e.g., Cloud One Help Desk) when identified issues are the CSP responsibility.

3.2.9.2 Monitor Jira tickets and provide CSP technical details as requested to include log files, error codes, etc.

3.2.9.3 Attend technical calls with CSP to troubleshoot identified issues.

3.2.10 **Sub-Task 2-10 - Certificate Management**

3.2.10.1 Ensure all application, system, and device certificates are managed from initial request and deployment through expiration date.

3.2.10.2 Track all certificate expiration dates, providing a Cloud One Certificate Status Report to the Program Manager semi-annually (as a minimum) starting 30 calendar days from task award.

3.2.10.3 Renew each certificate 30 calendar days prior to expiration using Cloud tools (e.g., AWS Certificate Manager) to streamline the management and utilization of certificates where feasible.

3.2.10.4 Document the certificate management process and procedures in the GDSS Cloud One CMP.

3.2.11 **Sub-Task 2-11 - Backup and Recovery**

3.2.11.1 Build and deploy backup and recovery solutions to back up system and operational data on a scheduled basis, accounting for all system and operational data locations (e.g., S3, database, web, application).

3.2.11.2 Execute and validate the backup and recovery solutions to include the ability to restore GDSS from backups within a Government directed timeframe.

3.2.11.3 Build and provide written instructions for the C2 Enterprise Help Desk (e.g., SIAOMS) to follow to back up or restore systems and/or data as required.

3.2.11.4 Build and deploy disaster recovery solutions to ensure the GDSS infrastructure, COTS/GOTS application, and all connections can be restored in the event of catastrophic failure of a component, service, or connection.

3.2.11.5 Document the solution, processes, and procedures in a Disaster Recovery Plan for Government review/approval within 45 calendar days of government request.

3.2.11.6 Validate and exercise all aspects of the disaster recovery plan at least annually to ensure it satisfies the Government's requirements.

3.2.12 **Subtask 2-12 - Testing**

The Contractor shall 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. As part of the cloud migration effort and transition to a DevSecOps strategy, the Contractor shall utilize a government approved automated software testing tool to accomplish testing. The Contractor shall conduct testing and complete the following tasks:

3.2.12.1 Produce and maintain test cases and deliver to the COR with each software release.

3.2.12.2 Produce and maintain a Software Test Report (STR) (CDRL A009) with the results of Contractor testing upon request.

3.2.12.3 Verify that the software meets the Software Requirements Specification (SRS) as provided by the government, (CDRL A013)/RSA.

3.2.12.4 Verify that the changed software does not adversely interfere with currently fielded hardware or accepted software baseline.

3.2.12.5 Verify that software meets test pass/fail criteria for each requirement contained in the SRS/RSA.

3.2.12.6 Perform testing (e.g., unit, system, regression, security, performance, load), and integrate automated testing into the processes when technically feasible and as approved by the PMO.

3.2.12.7 Perform static and dynamic performance testing, to include performance under load, as recommended by the developer and approved by the PM and COR. If performance degradation is identified during testing, the Contractor shall implement appropriate code modifications to eliminate that degradation. If performance degradation is determined to be a direct result of a requirement/design, the Contractor shall identify the requirement to the COR for resolution. The Contractor shall provide the results of performance testing to the COR with code delivery.

3.2.12.8 Perform static code analysis using approved tools, and dynamic security scans and probes using PMO approved software (ex. Fortify, WebInspect) prior to code delivery for any newly developed or updated software. The Contractor shall correct or mitigate security findings prior to final code delivery. The Contractor shall provide the security scan artifacts (CDRL A019) resulting from the security scans and probes to the COR with code delivery. In addition, the entire GDSS baseline shall be scanned once a quarter with the latest Fortify version and/or Rule Pack. Any vulnerabilities discovered that affect the current operational baseline shall be identified to the COR within 24 hours of discovery.

3.2.12.9 Perform external interface tests, as approved by the PM and COR. If connectivity to external entities is not feasible, the Contractor shall perform simulated tests to ensure message, file or service-based interfaces meet documented interface agreements.

3.2.12.10 Support regression testing upon porting the software to the COR-provided test Environment.

3.2.12.11 Conduct and participate with COR representatives in integrated testing, to include regression testing, to ensure the built capability is suitable for delivery to the COR as the test baseline (as defined in the Defense Acquisition Guidebook).

3.2.12.12 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.

3.2.12.13 Present a summary of completed efforts to achieve COR go / no-go decision for delivery of release.

3.2.12.14 Provide to the COR all testing artifacts (e.g., test results and Software Readiness Review (CDRL A023)) required to complete all acceptance testing.

3.2.12.15 Create, and update as needed, a Cloud One plan documenting how each area of testing will be performed, test results documentation approach, and the metrics that will be reported.

3.2.12.16 Manage Non-Production and Production test environments as required by the Government.

3.2.12.17 Implement automated testing to the fullest extent possible utilizing Government-approved automated testing tools to verify that the software meets test pass/fail criteria for each requirement as directed by the Government.

3.2.12.18 Provide Test Plans, Test Cases, Test Scripts, and Test Results for each software release in accordance with GDSS requirements.

3.2.12.19 Use blueprints and automated pipelines to the fullest extent possible to establish and validate Non-Production and Production environments, ensuring GDSS code and infrastructure changes can be securely promoted from the development environment to the test and Production environments.

3.2.12.20 Execute the following tests based on the software release requirements during the DevSecOps Build Phases: unit, smoke, integration, security, regression, performance/load (use load simulation tools to simulate users and monitor system performance in accordance with the Key Performance Parameters), stress (to assess the impact of changes on system performance and availability), failover, interface testing, end-to-end, to verify and validate the software release.

3.2.12.21 Support Government Acceptance Testing, interoperability testing, collaborative testing, and customer testing as directed by the Government.

3.2.12.22 Facilitate and participate in Test Readiness Reviews (TRRs), Production Readiness Reviews (PRRs), and Operational Readiness Reviews (ORRs) as directed by the Government.

3.2.12.23 Enter test defects into the Government provided test defect tracking tool.

3.2.12.24 Resolve test findings based on Government priority to fix test issues and defects.

3.2.12.25 Participate in Government test-related meetings as requested.

3.2.12.26 Perform data testing to ensure the data population process and programming logic are accurate and in accordance with Government-approved specification, to include validating data is replicated across data stores and/or caches as designed.

3.2.12.27 Perform Joint Interoperability Test Command (JITC) testing to include setting up environments, providing data, reporting metrics, etc., as directed by the Government.

3.2.13 **Subtask 2-13 - System Integration and Delivery**

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:

3.2.13.1 Prepare and deliver the configuration identification of the intended operational system.

3.2.13.2 Demonstrate that the software is integrated into the intended system configuration.

3.2.13.3 Perform the installation and fielding of the delivered system.

3.2.13.4 Prepare and deliver software releases and test results (CDRL A020) including all required components and documentation. The software shall include 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).

3.2.13.5 Generate the installation procedures (CDRL A022) (to include roll back and installation verification), sequencing, and schedule inputs associated with the version release or hardware installation. The Contractor shall implement automated software installation procedures as approved by the COR.

3.2.13.6 Generate a Software Version Description (SDV) (CDRL A016) for each GDSS component describing the changes made for the applicable release. This document shall be written in language understandable to the functional community.

3.3 **Task Area 3 – Security, Certification and Accreditation**

The Contractor is responsible for ensuring security, certification, and accreditation by updating the GDSS code to correct or mitigate high-priority findings, as identified by both the Project Manager and Contractor, using the latest version of Fortify, and adhering to software milestone release processes.

3.3.1 **Subtask 3-1 - Certification and Accreditation Support**

The Contractor shall provide security certification and accreditation support to the COR by providing the following services:

3.3.1.1 Adhere to all policies and procedures established for the authorization boundary of the Government-specified cloud development environment.

3.3.1.2 Create system documentation to support the Cloud One GDSS security assessment and authorization according to DODI 8510.01 Risk Management Framework (RMF) and the associated security controls as defined in DOD Instruction 8500.01 Cybersecurity (current version).

3.3.1.3 Correct or mitigate identified RMF-related security vulnerabilities and ensure the security testing results are available to the Government for review prior to delivery for inclusion in the RMF package.

3.3.1.4 Create and provide system artifacts as directed by the Government to support the RMF processes, for example:

(a) Architectural Diagrams

(b) Software Lists

(c) Ports and Protocols Matrix (PPSM)

(d) System Description

3.3.1.5 Create a Cloud One System Security Plan identifying all security processes, procedures, and tools implemented within the environment, to include routine activities such as refreshing control files, reporting status, etc.

3.3.1.6 Provide network, system architecture, and data flow diagrams for the Non-Production and Production systems and applications in Cloud One.

3.3.1.7 Support the GDSS Authority to Operate (AtO), Authorization to Connect (AtC), Interim Authority to Test (IATT), Certificate of Networthiness (CON), and Risk Management Framework (RMF) processes. Specifically, the Contractor shall produce and deliver a Threat Model (CDRL A018) and assist in preparation and review of other RMF documentation as required. This support is typically required in conjunction with releases or with annual security reviews but might occur during other security-related activities.

3.3.1.8 Advise and consult with the COR/Program Manager on matters of information and system security.

3.3.2 **Subtask 4-2 - Vulnerability Management**

The Contractor shall:

3.3.2.1 Maintain compliance with STIGs, CTOs, and security best practices by deploying software and configuration changes via an automated delivery, pipeline process.

3.3.2.2 Review applicable STIGs every 90 calendar days and identify any changes impacting the GDSS baseline to the Government with recommended remediation.

3.3.2.3 Deploy Government-approved remediation actions and baseline changes in the Non-Production and Production environments via an automated delivery, pipeline process.

3.3.2.4 Provide required level of support for cyber events in the Non-Production and Production environments to include Command Cyber Operational Readiness Inspections (CCORI), Cyber Protection Teams (CPT), Zero-Day responses and other cyber tasks as directed by the Government.

3.3.2.5 Deploy ACAS in compliance with DISA Best Practice Guide.

3.3.2.6 Update the plugin set on a daily basis via the approved DISA repository.

3.3.2.7 Provide the Government a Daily Scan Report and a Spot Scan Report each business day by 1200. Format to be provided by the Government.

3.3.2.8 Analyze security scans and build a security patch delivery to resolve all CAT I findings and any CAT II/III findings that have patches available.

3.3.2.9 Patch all CAT I findings within 21 calendar days, and CAT II/III findings when patches are available.

3.3.2.10 Validate security patches in Non-Production to ensure no impact to systems and applications.

3.3.2.11 Release security patches in Production via an automated delivery, pipeline process.

3.3.2.12 Review, analyze and respond to all CTOs as identified by the Government to include CTOs released on SIPRNet.

3.3.2.13 Generate Plan of Action & Milestones (POAM) for any CTOs or security findings that can't be resolved within 21 calendar days and/or specified due date.

3.3.2.14 Deploy/install security patches (e.g., OS, Application, Appliance) and upgrades via an automated delivery, pipeline process; upgrade administrative tools and utilities; and apply Time Compliance Network Order (TCNO), Information Assurance Vulnerability Management (IAVM), CTO, and other downward directed security patches.

3.3.3 Subtask 4-3 - GDSS Security Documentation Support

3.3.3.1 Reviews and Reports

The Contractor shall provide reviews and reports on proposed changes to system hardware, software, or environment for impacts to the GDSS security posture. Changes implemented by the Contractor to system hardware and software shall not violate the criteria for system accreditation.

3.3.3.2 Enhanced Security Products

The Contractor shall provide enhanced security for software code in its possession by preparing, maintaining, and following a Software/Product Protection Plan using AFP 63-1701 or current Government guidance as a guide. The plan and the Contractor's performance shall include the procedures and processes necessary to mitigate unauthorized access, tampering, and distribution of the application code. In addition, the plan and the Contractor's performance shall include the process and procedures the Contractor shall use to reduce the possibility of unauthorized access, tampering, unauthorized modification, to its software development and testing apparatus, such that it can provide reasonable assurance that these systems do not otherwise jeopardize the security and functionality of the products/software delivered to the COR.

At the completion of the contract, the Contractor shall obtain COR direction on the disposition of the GDSS software in its possession, regardless of the level of maturity and software derivative.

The Contractor's senior management representative shall submit to the Procurement Contracting Officer (PCO), as a condition for final payment, a written certification. The certificate shall state that to the best of the signor's ability, the signor certifies that the Contractor has complied with the COR's disposition instructions for the GDSS software in its possession.

3.4 Task Area 4 - Operations Support

3.4.1 Subtask 4-1 - Application Sustainment

The Contractor shall provide the same type of support for subtasks documented in Task Area 2 for sustaining the current, GDSS application capabilities in the cloud. Application sustainment includes activities such as modifications of the software to support software deficiencies; fact-of-life changes; upgrades for obsolete COTS software; the improvement of performance, usability, or any other quality attribute; integrating new functionality into current SOA interfaces (e.g., populating new fields into an interface service that was not previously populated or fixing software problem reports against current operational service baselines); deleting and

adding of functions to sustain warfighter capabilities (e.g., adding a new report/adding a new field to a screen); and correcting security vulnerabilities based on mission-driven PM and Functional Manager priorities/coordination in the form of monthly maintenance releases, hot fixes, and minor releases as tasked by the COR**.**

3.4.2 **Subtask 5-2 - Fielding Support**

The Contractor shall provide the following:

3.4.2.1 Research new equipment specifications for upgrade efforts.

3.4.2.2 Provide inputs and technical support related to the GDSS installation.

3.4.2.3 Provide direct installation support, to include troubleshooting, patch installations, Fielding System Checkout, etc., as requested by the PM.

3.4.2.4 Provide technical training to other GDSS Government or Contractor team members at the COR's request in preparation for software/system installations.

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

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

3.4.2.7 Deploy and maintain GDSS software releases (e.g., builds, emergency/hot/warm fixes) in the Non-Production and Production environments via an automated delivery, pipeline process, complying with STIGs, CTOs, DoD Security directives, FISCAM, and other regulatory guidance as required.

3.4.2.8 Confirm proper installation and operations of deployed software and infrastructure changes after each software release fielding.

3.4.2.9 Ensure all fielding activities are done via No Service Interruption (NSI) to minimize impact to users and interfaces.

3.4.2.10 Provide recommendations to minimize downtime as much as possible and obtain Government approval for a non-NSI installation if a NSI installation is not feasible.

3.4.2.11 Create and provide all required system documentation (e.g., user manuals, fielding instructions) prior to software release fielding.

3.4.2.12 Provide software application training for key technical personnel, functional help desk personnel, trainers, testers, video vignettes 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).

3.4.2.13 Maintain the Training Conduct Support Document, DI-SESS-81523B.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 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 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).

3.4.2.14 Create, design, and publish video vignettes to inform users of new build features as it is released to the application. (CDRL E003?)

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

3.4.2.16 Provide release notes, also known as (a.k.a.) Difference Training Guide, in "What's New" (CDRL A011) describing the features (new, changes, bug fixes) Create and manage the 'What's New' release notes. The Contractor shall provide a 'What's New' for each GDSS major or minor release. See sample document of Attachment 1. These release notes, also known as (a.k.a.) a Difference Training Guide, shall present all features in a release to include new or changed features and bug fixes. Each feature shall have a brief plain English overview and state the procedure or process on how it works. All fixes that effect any change in how the user operates the software shall also be identified, with an explanation of how it changes the utility (i.e. work-arounds replaced). Screen captures to visually demonstrate the look and use of the feature shall be included. Additionally, hyperlinks to additional or related information with the Help Files shall be added to enhance the customer experience and provide an easy access to related and relevant information. 'What's New' shall primarily live on-line; the user shall be able to download a full PDF version of the What's New document. The What's New information shall be incorporated into the appropriate Help File location with the following major release or as determined by the GDSS PMO.

3.4.3 **Subtask 5-3 - Technical Support**

The Contractor shall provide technical support (Tier 3) for GDSS application and systems and specialized equipment support, by accomplishing the following tasks:

3.4.3.1 Provide support during normal duty hours (PWS paragraph 3.2) and on-call after normal duty hours for the Production environments.

3.4.3.2 Have qualified support staff knowledgeable in all technical and functional aspects of GDSS and infrastructure on-call and available with access to the environment (e.g., connectivity, accounts) within 30 minutes of initial contact for the Production environments.

3.4.3.3 Respond with a knowledgeable technician onsite at the designated SIPRNet workspace within one (1) hour of initial contact for high priority events occurring in the IL6 / SIPRNet Production environments.

3.4.3.4 Work high priority tickets and Operational Reportable (OR) tickets 24x7 until resolution or a work around is identified and released by the Government.

3.4.3.5 Provide support during normal duty hours for the Non-Production environments.

3.4.3.6 Comply with all security requirements pursuant to DODD 5200.2-R, Personnel Security Program, DODI 8500-01 Cyber Security; DODD 8140.01, Cyberspace Workforce Management (dated 5 Oct 2020), Air Force Manual (AFMAN) 17-1303 (dated 12 May 2020), and Common Computing Environment Privileged User Requirements v1.2.

3.4.3.7 Ensure that all personnel assigned to work on the Contract requiring access to Government networks complete annual Information Assurance training by on-line Computer Based Training (CBT).

3.4.3.8 Ensure any member of the staff that needs the ability to deploy or modify anything within the GDSS Cloud One account has an IAT Level II "CompTIA Security+ ce" Certification as defined in DODD 8140.01 and AFMAN 17-1303.

3.4.4 **Subtask 5-4 – Technical Support**

3.4.4.1 Provide advanced technical services, formerly referred to as Tier 3, for Production environments and all Tiers for Non-Production environments to include all technology areas: network, operating system, database, Commercial off-the-Shelf (COTS)/Government off-the-Shelf (GOTS) applications, and cloud.

3.4.4.2 Troubleshoot network, system, database, COTS/GOTS application, and cloud issues; identify root cause(s), develop fix actions to resolve the immediate issue; and propose long-term strategies in order to avoid future re-occurrences to minimize user impact in the Production environments.

3.4.4.3 Track all trouble tickets in the enterprise ticketing system (currently Remedy) assigned to the developer and work the tickets in accordance with ticket priority and OR criteria.

3.4.4.4 Update all assigned tickets with troubleshooting steps and fix actions in accordance with the trouble ticket Standard Operating Procedures (SOPs).

3.4.4.5 Ensure all staff working tickets have all necessary accounts and credentials to access the Cloud One environments, COTS/GOTS applications, enterprise ticketing system, NIPRNet, SIPRNet, and designated Government SIPRNet workspace within 30 calendar days of task award.

3.4.4.6 Provide written instructions for MAF C2 Enterprise Help Desk (e.g., SIAOMS) support staff to monitor and troubleshoot the systems and applications 24/7 in the Production environments. Written instructions shall be clear, concise, and updated with each system and application release, and will be written at the Junior Technician level.

3.4.4.7 Coordinate with other programs' support teams as necessary to resolve issues involving / impacting other systems, establishing Associate Contractor Agreements (ACAs) as appropriate.

3.4.5 SubTask 5-5 – Technical Account Maintenance

The Contractor shall:

3.4.5.1 Update and implement account maintenance processes and procedures for the Non-Production and Production environments, ensuring these processes and procedures comply with all relevant security (e.g., STIG, SRG), financial (e.g., FISCAM), and programmatic requirements (e.g., account management procedures) to include Government approval for new/changed accounts.

3.4.5.2 Provide written instructions for the MAF C2 Enterprise Help Desk (e.g., SIAOMS) to create, track, expire, disable & delete functional and technical user and system accounts in the Production environments.

3.4.5.3 Create, track, expire, disable & delete functional and technical user and system accounts in the Non-Production environments.

3.5 Task Area 5 - Software Sustainment Environment

3.5.1 Subtask 5-1: Software Code Development and Testing

The Government will provide the Contractor with equipment and/or Cloud development environment for code development and testing.

The Contractor shall configure and manage the On Premise and/or Cloud development environments to support the tasks in this PWS. In addition, the Contractor shall:

3.5.1.1 Secure and logically separate the software sustainment environment from the Contractor's corporate administrative network.

3.5.1.2 Configure the software sustainment environment as closely as possible to the operational baseline configuration to include security patches and Standard Desktop Configuration (SDC).

3.5.1.3 Provide the capability to access AMC's Mobility Network (MobNet).

3.5.1.4 Host the COR-approved requirements tracking software on a secure environment accessible by a .com and .mil connection.

3.5.1.5 Provide a secured (access controlled) space with sufficient floor space, power, and HVAC to support the GFE.

3.5.1.6 Allow access to the software sustainment environment for Government personnel and other support Contractors as authorized by the COR. The Contractor shall provide work areas and wireless internet access for visiting Government and other Contractor personnel on an as required basis.

3.5.1.7 Provide the AWS and Cloud One expertise required to develop, operate, secure, and maintain the Development Cloud One environments to reliably and efficiently compile, build, test, and deploy secure code and instances.

3.5.1.8 The use of the software sustainment environment for purposes other than activities required to meet the requirements of this PWS and the contract must be authorized by the COR. Development servers and workstations will be managed and maintained by the Contractor. The Contractor shall maintain documentation for the configuration of the software sustainment environment and racks.

3.5.2 This task outlines the activities to migrate application development and deployment to a Software Factory. The Contractor shall, upon Government direction:

3.5.2.1 Provide a proposed Software Factory Migration Plan and updated Software Development Plan to show the vendor approach to migrate from the current development activities and processes to the Government-specified software factory, to include risks, timelines, and costs.

3.5.2.2 Migrate development activities and processes from the current GDSS application development environment (e.g., vendor hosted site, Cloud One) to the Government-specified software factory in accordance with the Government-approved Software Factory Migration Plan.

3.5.2.3 Utilize the Government-specified software factory environment, services, procedures, tools, and technologies to produce the GDSS code, tests, and associated artifacts to be deployed to Cloud One Non-Production and Production environments.

3.6 Task Area 6 – Modernization

The Contractor will adopt new technology and industry best practices that incorporate new and improved technology solutions for delivering value to the government.

All work conducted under this task shall be accomplished as directed by the Government in the form of Task Requirement Notices (TRNs.) The Contractor shall work with the Government to fill out TRNs. No work shall commence until the PCO has provided written approval to begin work. The use of TRN's can extended beyond Task Area 6 as needed.

1.6.1 Subtask 6.1 - Market Research and Prototyping

3.6.1.1 The Contractor shall evaluate COTS, Artificial Intelligence (AI), and other solutions to support and modernize GDSS applications, and other special equipment requirements.

3.6.1.2 The Contractor shall perform studies, 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 PMO.

3.6.1.3 The Contractor shall assist the Government by testing Government chosen products and making recommendations (CDRL B005).

3.6.1.4 The Contractor shall provide assistance when technical guidance is required. GDSS is a system of several sub-applications centered on different types of users.

3.6.1.5 The Contractor shall develop solutions to meet Government-directed changes and upgrades as required.

3.6.1.6 The Contractor shall adhere to industry best practices during development to include security engineering.

3.6.1.7 GDSS Applications – The Contractor shall provide standalone applications with the capability to operate on multiple operating systems, e.g. iOS, Android, Windows, etc. Applications will be used in multiple environments, for example, Electronic Flight Bag (EFB) and onboard aircraft. In addition, the Contractor shall provide a mobile GDSS application that operates in a connected and disconnected mode with touch screen and voice navigation (mouse/keyboard free). These applications shall be based on user community requirements and shall be created and delivered with an agreed upon schedule.

3.6.1.8 The Contractor shall support and build application program interfaces (API) to data lake platforms or other data exposure platforms, e.g. Unified /data Library (UDL), COTS products, or as directed by GDSS PMO.

3.6.1.9 The Contractor shall provide development teams to work special projects separate from the Sustainment/ Development team. Projects shall be assigned by TRN per the PCO and are separate from beyond normal sustainment activities. Teams shall utilize Agile and DevSecOps methodology, JIRA and the same requirement and change management tracking practices as the Sustainment team.

3.6.1.10 **Completed projects may continue to remain as standalone projects and remain with a special projects**, **or migrate to the sustainment team for future sustainment after final delivery and production implementation**. T**his management shall be determined by the COR in coordination with the GDSS PMO and Contractor.**

3.7 Task Area 7 – Decommission On-Premises Environment(s)

This task outlines the activities to decommission the on-premises development environment. The Contractor shall, upon Government direction:

3.7.1 Provide a plan to decommission the on-premise development environments to include cost, schedule, and risk. Upon Government decommission plan approval, take steps to decommission any on-premises development environments.

3.7.2 Coordinate with the Government Equipment Custodian for return of all Government Furnished Equipment (GFE) for the on-premises development environment within 60 calendar days of the Government-approved decommission date.

3.7.3 Coordinate with the Government for turn-in of any development environment specific software licenses.

3.7.4 Coordinate with the Government to turn-off any circuits or other connections put in place by the Government to support the development environment.

4. SERVICES SUMMARY (SS)

The following Services Summary identifies the performance objectives and performance thresholds for critical tasks associated with providing support services for this requirement. The performance threshold briefly describes the minimum acceptable levels of service required for each performance objective. These thresholds are critical to mission success. The absence of any performance objective and threshold from the SS shall not detract from its enforceability or limit the Government's rights or remedies afforded under this contract.

Performance Objective	PWS Para.	Performance Threshold	Method of Surveillance
SS 1. 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	Performance is acceptable when there is 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.	100% Inspection
SS 2. 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	Performance is acceptable when there is no more than three rewrites per quarter resulting from inaccurate, incomplete, or unsupported information.	Random Sampling
SS 3. All reports and Documents (CDRL B001-B006 and B007-B009) except 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	Performance is acceptable when there is no more than one rewrite per month resulting from inaccurate, incomplete, or unsupported information.	100% Inspection
SS 4. 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	Performance is acceptable when there is 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.	100% Inspection
SS 5. All Procedures and Description Computer Software End Items (C009)	3.1.2, 4	Performance is acceptable when there is no more than eight re-deliveries of CCB code fixes per quarter.	100% Inspection

provided are free from critical errors.		No more than three Must Fix test findings per major release.	
SS 6. 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	Performance is acceptable when there is no more than three rewrites per quarter resulting from inaccurate, incomplete, or unsupported information.	100% Inspection
SS 7. Data deliverables are produced using prescribed formats, software tools, and 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.	3.12, 4	Performance is acceptable when there is no more than two inaccuracies per month for cross-referencing 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.	Random Sampling
SS 8. Level of expertise, coordination, and support necessary to accomplish the contract in a responsive, satisfactory, and timely manner is provided.	3, 3.7	Performance is acceptable when there is no more than one valid customer complaint per month in performance of required tasks. All complaints are resolved not later than one (1) business day beyond the PM/Contractor agreed-to time period.	Customer Complaint Record
SS 9. Effective corrective actions ensure noted discrepancies are corrected, COR follow-ups are precluded, and corrective actions eliminate recurrence of the same or similar discrepancies.	3.4.4,	Performance is acceptable when all deficiencies are corrected not later than one working day beyond the agreed-to time period per month.	Random Sampling
SS 10. 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.	100% Inspection
SS 11. 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	100% Inspection

		Contractor. No instances of late verbal notices per month.	
SS 12. 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.	100% Inspection
SS 13. 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.	100% Inspection

* A valid complaint is one that is consequential to the successful performance of the requirement for an issue that was not corrected in a reasonable amount of time and adversely impacted performance, schedule, and/or cost.

5. GENERAL REQUIREMENTS

5.1 Place of Performance

The primary place of performance is Contractor's facility and Scott AFB. Additional temporary duty (TDY) locations are CONUS/OCONUS as mission and contract requirements dictate. The Government will provide workstations for necessary Contractor employees at Scott AFB. Telecommuting may be allowed/required on a limited basis, at the Government's discretion, and shall be pre-coordinated with the respective Government COR. If office space becomes limited at Scott AFB, then hoteling (a method of office management in which workers dynamically schedule their use of workspaces such as desks, cubicles, and offices) may become an alternative approach to the more traditional method of permanently assigned seating. If this becomes necessary, the COR will coordinate with the Contractor Program Manager.

5.2 Duty Hours

The Contractor shall support the following duty hours:

- Technical support shall be 24/7/365 for high priority trouble tickets as defined by the AFLCMC/HBM Operating Location 2 (OL-2) Consolidated Operational Reportable (OR) Instructions.
- The Contractor shall be available to correspond and attend meetings during normal Government duty hours (meetings may be held at Scott AFB [exact bldg, location, TBD] and Contractor's facility). Government duty hours are 0700 -1700 CST Monday through Friday, except for Federal holidays.
- The Contractor will operate during normal Government duty hours unless the PM directs a change to accommodate events such as installation support. In addition, the Contractor shall provide telephone/on-site, on-call functional support 24/7/365. On-site support is required for SIPR and for NIPR, if telephone or on-line support cannot resolve trouble ticket. See Section G of the task order for billing instructions.

5.3 Materials

The Contractor shall provide any materials, to include software licenses, to accomplish the performance requirements IAW FAR 31.205-26 to the COR prior to purchase.

Purchases of materials in a single order below the micropurchase threshold (see FAR 2.101 Definitions) are not required to be competed but shall be procured at the best market prices obtainable and submitted to the COR. The contractor shall provide documented competition for the entire order

to the COR prior to proceeding with the purchase. Any discounts and/or rebates on materials obtained by the Contractor shall be credited to the Government.

The COR and Program Office will review the documentations and forward such documentations to the PCO for approval/disapproval within five (5) business days.

5.4 **Travel**

Travel by Contractor personnel may be required in support of this contract. Contractor travel costs shall be IAW FAR 31.205-46. The Contractor shall travel using the lowest cost mode transportation commensurate with the mission requirements. When necessary to use air travel, the Contractor shall use the tourist class, economy class, or similar accommodations to the extent they are available. Costs for lodging, meals, and incidental expenses may be based on per diem. Upon the notification of any required travel, the Contractor shall provide the cost estimate to the CO for approval.

The Contractor shall submit a travel itinerary and estimated cost for approval by the CO and confirmation on availability of funds from the CO not later than ten 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 IAW FAR 31.205-46. 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 A010). Travel will be reimbursed at allowable cost in accordance with the FAR 31.205-46, Travel Costs, in effect on the date(s) the travel is performed.

Travel shall not exceed obligated funding on the associated line item IAW AFLCMC/HBK-H002: Time and Materials - Funding by Increment (JANUARY 2022).

All travel reimbursement receipts shall be submitted to the COR within 10 days after completion of the trip.

5.5 **Transition**

The Contractor shall provide a Transition Management Plan (CDRL A006) for the 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 DevSecOps 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. Weekly status briefings will be provided to the COR and associated Contractors throughout the transition period. The Contractor shall accomplish the following phase-in transition tasks within the transition period of performance as specified by the contract.

- Implement the proposed methods, processes, procedures, and tools as described in the approved transition plan.
- Assume responsibilities as outlined in the tasks of this PWS. Technical Support responsibilities**.**

When there is a change in Contractor upon award of a new contract or at any time the operation reverts to the DOD, there will be a phase-out period associated with the transfer of records/data

by the Contractor (incumbent). The Contractor shall provide a Transition Management Plan (CDRL A006) for the phase-out strategy describing the method of transferring responsibility for tasks described in the PWS. The Phase-Out Plan will detail how all tasks will be transferred to the successor. The incumbent and successor Contractor shall cooperate during phase-out orientation that will begin immediately after follow-on contract award or whenever the CO directs the changeover. During the phase-out period, the incumbent Contractor shall be fully responsible for PWS performance requirements and cooperate with the COR/COR and associated Contractors to the extent required to permit an orderly changeover to the successor. The incumbent Contractor is responsible for protecting government Intellectual Property, while the Government remains responsible for facilitating GFE transfer from the incumbent to the successor Contractor. Bi-weekly status briefings will be provided to the COR/COR and associated Contractors throughout the transition period.

Within six months prior to contract completion, the Contractor shall preserve and make available to the COR copies of all records and other documentation, established or acquired under this contract, regarding performance of the work required by this contract. Within 60 calendar days prior to the contract completion, the Contractor shall provide to the COR the following information:

- Transition Management Plan (CDRL A006)
- Complete backup of all contract and contract related data stored on each employee's hard drive or servers along with any global data. List of all GFE and COTS utilized in support of this task.
- Soft and hard copies of all procedures and documentation generated as part of this task.
- Obtain Government direction on the disposition of the GDSS software in its possession, regardless of the level of maturity and software derivative.
- Obtain PM/COR direction on the disposition of the GDSS GFE in its possession.

Contract data shall not be corrupted, changed, or altered such that it would cause damage to the Government. This includes hardware and software configurations on all platforms.

5.6 Data Rights

All software, source code, computer software documentation, enhancements, and technical data shall be written with Government funds and shall result in unlimited data rights; no restrictive data rights assertions shall be permitted under this Task Order in accordance with DFARS 252.227-7013, 252.227-7014, and 252.227-7015.

5.7 Security Management and Security Clearances

All personnel assigned to this contract shall be United States citizens and shall possess a minimum of a SECRET Security Clearance. 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.

When obtaining security clearances, the Contractor shall comply with:

- DoD Instruction (DoDI) 5220.31 National Industrial Security Program
- DoD Manual (DoDM) 5200.01 Vol 1 DoD Information Security Program: Overview, Classification, and Declassification
- DoDM 5200.01 Vol 2 DoD Information Security Program: Marking of Information

- DoDM 5200.01 Vol 3 DoD Information Security Program: Protection of Classified Information

Facility and employee security clearances are obtained according to DOD 5220.22-M (National Industrial Security Program Operating Manual). This manual includes specific requirements for the handling of classified information, security clearance, control of areas, visitor control procedures, subcontractors, vendors and suppliers, consultants, parent-subsidiary and multiple facility organizations, sensitive compartmented and Communications Security (COMSEC) information, overseas operations, security requirements for automated information systems, and operations security (OPSEC). This includes clearance procedures, visitors, inspections, violations, education, classification, international security programs, and OPSEC. Contractors may be required to conduct facilities security checks.

All personnel shall follow all DoD Controlled Unclassified Information (CUI) policy. All DoD CUI must be controlled until authorized for public release in accordance with:

- DoDI 5230.09 Clearance of DoD Information For Public Release
- DoDI 5230.29 Security and Policy Review of DoD Information for Public Release
- DoDI 5400.04 Provision of Information to Congress
- DoDM 5400.07 Freedom of Information Act (FOIA) Program
- Official DoD information that is not classified or controlled as CUI will also be reviewed prior to public release in accordance with DoDIs 5230.09 or 5230.29.

5.8 Cyber and Information Security Requirements

5.8.1 Network and Computer Security

The Contractor shall be knowledgeable with the Air Force Manual (AFMAN) 17-1301, “Computer Security,” as well as AMC system security policies, and deliver software it delivers to the Government that is compliant with those policies.

5.8.2 Information Assurance (IA)

The Contractor shall comply with all security requirements pursuant to

- DoDI 5200.02-R, "DoD Personnel Security Program"
- DoDI 8500.01, "Cybersecurity"
- DoDM 8570.01-M, "Information Assurance Workforce Improvement Program"
- AFMAN 33-285, "Information Assurance"

All Contractor personnel assigned to work on the contract who require access to Government networks shall complete Annual Information Assurance training by on-line CBT. The Contractor is responsible for having an Information Assurance Training (IAT) Level II “CompTIA Security+ ce” Certification as defined in DoD 8570.01M and AFMAN 33-285 for Functional Help Desk personnel at full performance date of contract.

5.8.3 Antiterrorism 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, “Antiterrorism Standards”. 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 available through myLearning and provided at https://lms-jets.cce.af.mil, Force Protection Course (ZZ133079).

5.8.4 Operations Security (OPSEC)

The Contractor shall ensure OPSEC is incorporated into the appropriate area of the contract IAW:

- DoD Directive 5205.02E, "DoD Operations Security (OPSEC) Program"
- DoD Instruction (DoDI) 5200.01, "DoD Operations Security (OPSEC) Program
- AFI 10-701, "Operations Security"

The Contractor shall flow down all OPSEC requirements to subcontractors that handle Critical Information (CI). CI is defined as, "Specific facts about friendly intentions, capabilities, and activities needed by adversaries for them to plan and act effectively so as to guarantee failure or unacceptable consequences for friendly mission accomplishment."

5.8.5 **Access to Government Automated Information Systems**

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. When the period of performance is complete or Contractor personnel leave work on this project they will have five (5) business days to terminate all their network user account and to return all access cards and base identification badges. All Contractor and subcontractor personnel must have the appropriate security clearance before being authorized access to Federal Government computers and networks.

5.8.6 **Safeguarding Classified and Unclassified Information**

The Contractor shall meet Air Force standards for storing, processing, and handling classified information and systems, IAW:

- AF 16-1404, Information Security Program: Overview, Classification, and Declassification
- DODM 5200.01

The Contractor shall complete the online OPSEC Awareness course, understanding the need to protect unclassified information about operations and personal information. Additionally, all resources (e.g., maps, publication/instructions, photos) provided by the Government to assist the Contractor in the performance of their contract, shall be surrendered upon termination of employment or the end of the contract performance period.

5.8.7 **Controlled Unclassified Information (CUI)**

The Contractor shall be compliant to National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 in accordance with DFARS 252.204-7008. The Contractor shall comply with:

- DoDI 5200.48_DAFI16-1403, Controlled Unclassified Information,
- DoDM 5200.01, Vol 1
- AFMAN16-1404, Vol 1, Air Force Information Security Program, and
- DoDM 5400.07
- AFMAN 33-302 Air Force Manual, DoD Freedom of Information Act (FOIA) Program.

The Contractor shall monitor CUI aggregation and compilation based on the potential to generate classified information pursuant to security classification guidance addressing the accumulation of unclassified data or information. The Contractor shall distribute controlled unclassified information IAW:

- DoDI 3200.14, Principles and Operational Parameters of the DoD Scientific and Technical Information Program, and
- DoDI 2040.02, International Transfer of Technology, Articles, and Services

The Contractor shall properly mark all such documents:

- IAW DoDI 5230.24, Distribution Statements on Technical Documents

Technical documents not subject to distribution are defined in:

- DoDI 5230.24, DoDD 5230.25, and
- DoDM 5010.12-M, Procedures for the Acquisition and Management of Technical Data

5.8.8 **Disseminating Scientific and Technical Information (STINFO)**

The Contractor shall use DAFI 61-201, Management of Scientific and Technical Information (STINFO) and DoDI 5230.24, Distribution Statements on DoD Technical Information, when developing, reviewing, or assisting the US Government and other supporting Contractors, to identify any "sensitive" media that should not be placed into the Public Domain (e.g., Classified, CUI), as well as ensuring applicable Distribution Statement, Handling and Destruction Notice, Warning Statement (for technical information with Space/Military Application under the International Traffic Arms Regulation (ITAR) or the Export Arms Regulation for dual-use technologies), along with the Expanded Exemption Statement are applied. The Contractor shall consult with the GDSS PMO to determine the appropriate Distribution Statement for the media. From the time of creation by the Contractor, the Contractor shall properly mark, properly handle, secure, and dispose of any sensitive media in the Contractor's immediate control. The Contractor shall advise/alert US Government, and other supporting Contractors of these requirements, for any sensitive media received which is not appropriately marked.

5.8.9 **Handling of Non-Public Information**

In performance of this contract, the Contractor may have access to Department of Defense (DOD) information. The Contractor agrees:

(e) To use and protect such information from unauthorized disclosure IAW DOD Instruction 8582.0: Security of Non-DoD Information Systems Processing Unclassified Nonpublic DoD Information;

(f) 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;

(g) To comply with other current Federal and DOD information protection and reporting requirements for specified categories of information (e.g., medical, proprietary, critical program information (CPI), personally identifiable infom1ation, export controlled);

(h) To obtain permission of the Government Requiring Activity before disclosing/discussing such information with a third party; and

(i) To return and/or electronically purge, upon Government request, any DOD information no longer required for Contractor performance; and (f) to advise the PCO and/or COR of any unauthorized release of such information.

5.8.10 **Periodic Government Inspections**

The Contractor (and its subcontractors) shall authorize Government inspections and reviews of its unclassified IT environment where DOD information is resident or transiting to assure compliance with DOD cyber security requirements throughout the contract performance period. The Contractor shall be responsible for taking corrective action based upon the impact and severity of identified weaknesses. The Government will limit inspections to a maximum of one per year. The Contractor shall allow follow-on visits, if requested, to confirm resolution of any significant weaknesses identified during the inspections.

5.8.11 **Remote Access**

Contractor Furnished Equipment (CFE) employed for remote access to a Government network must meet or exceed equivalent GFE cyber security computing requirements. All CFE (hardware and software) employed to access these environments shall meet the following minimum Government cyber security requirements and provide periodic certification of compliance as a pre-requisite to being granted network access.

- Use of personally owned systems is prohibited;
- Operating systems and applications must be configured for compliance with the applicable Security Technical Implementation Guides (STIGs);
- DOD approved anti-virus and anti-spyware software must be installed and signatures must be configured to automatically update on a daily basis;
- DOD approved host-level firewall must be utilized and configured to permit traffic by exception only, dropping all other traffic. If the host-level firewall provides intrusion detection or prevention, the signatures or rules must be updated at the same intervals as the anti-virus software.
- Computers must be Information Assurance Vulnerability Management (IAVM) compliant;
- Computers must be scanned with the currently approved DOD scanner solution at a minimum of every 30 calendar days. All vulnerabilities must be remediated and reported to the cognizant Information Assurance Manager;
- Contractor employees must possess a current Government issued Common Access Card (CAC) and install Government certified CAC readers; and
- Verification of compliance with these requirements must be provided to an appointed government representative on a monthly basis.

5.8.12 **Non-Disclosure Agreements**

The Contractor shall execute Non-Disclosure Agreements (NDA) as Contractor personnel will work with sensitive or proprietary information provided from the Government, other contractors, and firms not having Government contracts, academic institutions, and other nonprofits.

The non-disclosure restriction shall be included in all subcontracts, teaming arrangements, and other agreements calling for performance of work. The purpose of these agreements is to prevent disclosure of sensitive Government information the Contractor may be exposed to through performance of this contract. These agreements are not intended to protect information which is available to the Government or to the Contractor from other sources and which have been furnished voluntarily without restriction.

Any contract employee granted access to Classified under this contract must have an SF-312, Classified Information Nondisclosure Agreement, on file. Government reserves the right to review the SF- 312 at any time.

Copies of signed NDAs shall be submitted to the CO within 48 hours of the hire date. The contractor is required to provide to the Government an NDA containing the information provided in Appendix A.

5.8.13 **Protecting Government Intellectual Property**

At the completion of the contract or when turning-in Government IT equipment to the Government, the Contractor shall not remove, 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 PCO. This requirement is invoked whether the data, files, etc. are placed there by the Contractor employees in 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 Government. Failure of the Contractor to comply with this paragraph may subject the Contractor to breach of contract, civil penalties, criminal charges, or all three.

Upon delivery of the final version release or other deliverable under this contract, the Contractor shall deliver to the COR and/or at the direction of the Government transfer to another Contractor, the following:

- 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.
- 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 contact and/or documents prepared during contract performance for use under the contract.
- Technical orientation of GDSS system to include definition and description of all modules. Source code, object code, database applications, and permissions to access the source, object code, and ORACLE database.
- All Government furnished hardware – servers, PCs, laptops, monitors, external hard drives, cabling, switches, routers, and all peripheral devices.
- 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.

.

5.8.14 **Privacy Act**

Work on this project requires that personnel have access to Privacy Information. Personnel shall adhere to the Privacy Act, Title 5 of the U.S. Code, Section 552a and applicable agency rules and regulations. Refer to AFI 33-332 (Air Force Privacy and Civil Liberties Program).

5.8.15 **Contractor Consent to Background Checks**

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 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 this section. Furthermore, nothing in this clause shall excuse the Contractor proceeding with the contract as required**.**

5.8.16 Proper Employee Credentials

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

4.7.18 Future Cyber and Information Security Requirements

The Contractor shall comply with any new, changed, or updated requirements of which the Government will inform the Contractor along with expected date(s) for meeting compliance standards.

5.9 Incident Handling

5.9.1 Reporting Requirements

The Contractor shall notify the PCO and the COR within 48 hours of any incident involving the actual or suspected compromise/loss of classified information to enable the Government to conduct immediate assessments of potential impact pending formal inquiry/investigation. Actual or suspected compromise of Covered Defense Information will be reported IAW DFARS 252.204-7012.

The Contractor shall provide an initial incident report to the Defense Cyber Crime Center (DC3) as soon as possible upon discovery of any suspected cyber intrusion events on the Contractor's (or its subcontractors') unclassified information system(s) or network(s) where DOD information is resident or transiting. The initial incident report shall be provided even if some details are not yet available, with follow-on detailed reporting to DC3 within 72 hours. Reportable cyber intrusion events include the following:

- A cyber intrusion event involving possible data exfiltration, manipulation or unauthorized disclosure of any DOD information resident on or transiting the Contractor's (or its subcontractors') unclassified information systems or networks;
- Intrusion activities that allow unauthorized access to the Contractor's unclassified information system(s) or networks(s) on which DOD information is resident or transiting.

5.9.2 Incident Report Submission/Content

The Contractor shall submit unclassified incident reports to DC3 via the Defense Industrial Base Network (DIBNet) Portal (https://dibnet.dod.mil). The incident report shall include, at a minimum, the following information:

5.9.2.1 Company name

5.9.2.2 Data Universal Numbering System (DUNS) Number

5.9.2.3 Facility CAGE code

5.9.2.4 Facility Clearance Level (Unclassified, Confidential, Secret, Top Secret, Not Applicable)

5.9.2.5 Company point of contact information (name, position, telephone, email)

5.9.2.6 U.S. Government Program Manager point of contact (name, position, telephone, email)

5.9.2.7 Contract number(s) or other type of agreement affected or potentially affected

5.9.2.8 Contracting Officer or other type of agreement point of contact (address, position, telephone, email)

5.9.2.9 Contract or other type of agreement clearance level (Unclassified, Confidential, Secret, Top Secret, Not Applicable)

5.9.2.10 Impact to Covered Defense Information

5.9.2.11 Ability to provide operationally critical support

5.9.2.12 Date incident discovered

5.9.2.13 Location(s) of compromise

5.9.2.14 Incident location CAGE code

5.9.2.15 DoD programs, platforms or systems involved

5.9.2.16 Type of compromise (unauthorized access, unauthorized release (includes inadvertent release), unknown, not applicable)

5.9.2.17 Description of technique or method used in cyber incident

5.9.2.18 Incident outcome (successful compromise, failed attempt, unknown)

5.9.2.19 Incident/Compromise narrative (Ex: Chronological explanation of event/incident, threat actor TTPs, indicators of compromise, targeting, mitigation strategies, and any other relevant information to assist in understanding what occurred)

5.9.2.20 Any additional information

In the event of an intrusion or potential intrusion, the Contractor agrees to allow follow-on actions by the Government to further characterize and evaluate the suspect activity. The Contractor acknowledges that damage assessments might be necessary to ascertain intruder methodology and identify systems compromised as a result of the intrusion. The Contractor acknowledges that in certain cases a complete forensic analysis might be necessary to ascertain intruder methodology and identify systems compromised as a result of the intrusion. Once an intrusion is identified, the Contractor agrees to take all reasonable and appropriate steps to preserve any and all evidence, information, data, logs, electronic files and similar type information (reference NIST Special Publication 800-6 1: Computer Security Incident Handling Guide, (current version)) related to the intrusion for subsequent forensic analysis so that an accurate and complete damage assessment can be accomplished by the Government. The Contractor is not required to maintain an organic forensic capability but shall preserve data (e.g. removing an affected system, while still powered on, from the network meets the intent of this

requirement) and all actions documented until forensic analysis can be performed by the Government or mutually agreed upon third party (e.g. Federally Funded Research and Development Center (FFRDC), commercial security Contractor, etc.). Any follow-on actions shall be coordinated with the Contractor via the COR.

5.9.3 **Law Enforcement/Counterintelligence**

In the event of a known or potential intrusion, the Contractor shall consent to responding counterintelligence or law enforcement investigative agency requests to apply forensic analysis tools to Contractor information systems affected by the intrusion, including monitoring tools, imaging tools, and any other techniques that the agency seeks to apply to effectively analyze the intrusion. The Contractor shall allow the responding counterintelligence and/or law enforcement investigative agency to image affected systems, including systems containing proprietary information. Nothing in this contract shall limit the ability to conduct law enforcement or counterintelligence activities, or other activities in the interest of the Government.

5.9.4 **Security Training**

Contractor employees assigned to AFLCMC and utilizing its enterprise networks shall attend/complete security training as prescribed by DOD and Air Force instructions. At a minimum this includes:

- Employee Initial Security Training
- Annual Security Awareness Training
- Operations Security (OPSEC)
- DOD Antiterrorism Level 1 Training,
- Active Shooter Training
- Personally Identifiable Information (PII) Training
- Emergency Operations
- Any Security Stand Down Day Training scheduled by the Commander
- Security training established by their respective government security offices and/or installations

5.9.5 **Software Sustainment Environment**

The Contractor's software sustainment environment shall comply with the security and technical requirements detailed in paragraph 2.7.

5.9.6 **System Design, Information System Security Engineering Principles; DOD, NIST Directives**

The Contractor shall employ information system security engineering during any/all changes to the system architecture. Such modifications will be made in compliance with all analogous or interfacing cyber security component(s) of the Department of Defense Information Network (DODIN) Architecture and will be designed to make maximum use of the DOD enterprise cyber security capabilities and services. As part of the Contractor's change control process, participation by an Information System Security Engineer or a qualified cyber security subject matter expert (SME) shall evaluate the impact of each change on security.

5.9.7 **DoD Assessment and Authorization**

The Contractor shall be responsible for establishing system documentation to facilitate the security assessment and authorization of the system according to DODI 8510.01 Risk Management Framework and the associated security controls as defined in DOD Instruction 8500.01 Cybersecurity (current version). The Contractor shall update the DOD Enterprise

Mission Assurance Support Service (eMASS) system as required and provide supporting cyber security documentation for upload as artifacts in eMASS.

5.9.8 **Software Assurance and Security Engineering Practices**

In coordination with the Government, the Contractor shall design, build and implement secure applications and configurations through applying applicable DOD STIGs, checklists, vendor security guidance, industry best practices, and applicable vendor product security patches. Applications shall be in compliance with DOD Instruction 8500.01 Cybersecurity (current version) and DODI 8551.0l Ports, Protocols, and Services Management (PPSM) (current version). The Contractor shall leverage, to the maximum extent possible, automated tools to identify and remediate vulnerabilities or weaknesses in the application design/coding, such as those described in Common Weakness Enumeration/System Administration, Networking, and Security Institute (CWE/SANS) TOP 25 Most Dangerous Software Errors (http://www.sans.org/top25-software-errors/) and Open Web Application Security Project (OW ASP) Top Ten (https://www.owasp.org) that could be exploited by unauthorized sources.

The Contractor's Information System Security Engineer shall participate in Government and Contractor formal and informal design reviews to identify potential security weaknesses, deficiencies, and/or vulnerabilities in the design. The Contractor's Information System Security Engineer shall also include appropriate security requirements as part of the requirements traceability matrix and shall be evaluated as part of the security assessment. As part of the Contractor's change control process, the Information System Security Engineer or a qualified cyber security SME shall evaluate the impact of each change on security. The Contractor shall document the results of this evaluation to support risk management processes.

5.9.9 **Non-Secure Software**

If the Government determines, after a security audit (e.g. security assessment), that software delivered under this acquisition is non-secure, the Government will provide written notice to the Contractor of each non-conformity. Software shall be "non-secure" under this contract if it contains a software error listed on the current approved version of the CWE/SANS TOP 25 (https://www.sans.org/top25-software-errors/) or a web application security flaw listed on the current approved version of the OW ASP Top Ten. (https://owasp.org/www-project-top-ten).

The Contractor shall have 30 calendar days after receipt of such notice (Remedy Period) to remedy each non-conformity by modifying/replacing and redelivering the software to the Government; or shall notify the Government within 15 calendar days as to why the remedy cannot be implemented in 30 calendar days and propose a timeline for correction. If the Government determines, after a security audit following a Remedy Period, that the redelivered software is non-secure, and thus non-conforming, the Government may reject the delivery, provide notice of the non-conformance, and document the Contractor's performance record. Alternatively.

5.9.10 **Malicious Code Warranty**

The Contractor represents and warrants that upon delivery to the government the software shall be free from all known computer viruses, worms, time-outs, time bombs, back doors, disabling devices and other harmful or malicious code intended to or which might damage, disrupt, inconvenience or permit access to the software user's or another's software, hardware, networks, data or information that the Contractor reasonably should have known.

Do not send identified malicious code to the Contracting Officer, COR, Program Manager, or any other member of the Government. Contractor/Subcontractor identified malicious code shall be handle in accordance with DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, and any other applicable clauses on the contract.

5.10 **Contractor Access**

5.10.1 **Contractor Identification/Badges**

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

The Contractor shall 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 and company name and be clearly and distinctly marked as Contractor. 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.

5.10.2 **Access to Government Facilities (Contractors not Authorized a DoD Common Access Card)**

Contractor employees will be authorized unescorted access to the installation using locally produced Defense Biometric Identification System (DBIDs) credential issued by the installation security forces visitor control center upon receipt of a favorable background check. The Contractor shall follow Contractor entry control requirements outlined in AFI 31-113, Installation Access Control and the local Integrated Defense Plan and command/local directives. The Contractor is not authorized escort authority for the installation. Any employee not in possession of a DBIDs credential must be escorted by the sponsoring organization. Individual Contractor DBIDs cards must be immediately returned to security forces upon termination of employment or completion of the contract when installation access is no longer required.

5.10.3 **Access to Installations (Contractors with DoD Common Access Card)**

The Contractor shall ensure a CAC is obtained by all Contractor/Subcontractor personnel who require access to DoD computer networks/systems, for DoD facility entry control and/or for physical access to facilities and buildings to perform tasks under the contract. The Contractor shall provide a list of Contractor/Subcontractor personnel who require a CAC to the COR. The Government will provide the Contractor instruction on how to complete a Contractor Verification System (CVS) application and notify the Contractor of approval/ disapproval of Contractor/Subcontractor personnel application. Contractor/Subcontractor personnel shall obtain the CAC from the local Real Time Automated Personnel Identification Documentation System (RAPIDS) issuing facility (usually the Military Personnel Flight (MPF)). The Contractor shall immediately report a lost or stolen CAC as directed by local Government policy. The Contractor shall notify the PCO and COR of any change to the list of Contractor/Subcontractor personnel who require a CAC and provide an updated list within five (5) business days. The Contractor shall return a CAC within five (5) business days once Contractor/Subcontractor personnel no longer require computer network/system access and/or facility access. The Contractor shall return an expired CAC within five (5) business days after the expiration date. The Contractor shall return any and all CACs within five (5) business days after completion/termination of the contract as directed by local Government policy.

The GDSS Program Management Office, AFLCMC OL-2/HBMSA, or its successor organization, will assist Contractor personnel in processing the necessary DOD forms to obtain base or area badges for access to Government facilities.

5.10.4 **Contractor Registration of Vehicles**

All Contractor or Contractor employees' vehicles used for the performance of this contract shall comply with all local, state and federal regulations, including, but not limited to, valid vehicle registration and proof of current insurance. Additionally, any pass shall be surrendered to Security Forces upon demand to positively identify a person's need to be on the installation.

5.10.5 **Access to Government Facilities with Controlled or Restricted Areas**

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, the Government may direct the Contractor to leave the controlled or restricted areas at any given time.

5.10.6 **Access to Government Facilities with Controlled or Restricted Areas for Replacement Contractor Personnel**

The unit requesting contract support will continuously escort replacement Contractors not initially possessing the proper clearances and requiring entry to controlled or restricted areas. Replacement Contractor must submit paperwork within seven (7) business 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 shall 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.

5.10.7 **Contractors Working in Controlled or Restricted Areas**

Only Contractor personnel with proper authority and qualifications shall enter a controlled or restricted area. Certain facilities require the issuance of an AF Form 1199CD, USAF Restricted Area Badge. The government, at any time, may revoke the AF Form 1199CD. The procedures for the issuance of an AF Form 1199CD are contained in Scott Air Force Base Instruction (SAFBI) 31-101, Security Integrated Defense. The Contractor shall not escort other Contractor employees within controlled or restricted areas. In addition, Contractors shall fulfill, maintain, and comply with all security requirements contained in SAFBI 31-101, Installation Security Instruction.

The Contractor must have an issued AF Form 1199CD; work on base a minimum of four (4) days a week (must have an assigned workspace on base). In addition, Contractors must fulfill, maintain, and comply with all security requirements IAW DAFI 31-101, Integrated Defense (ID), and command/local directives.

5.10.8 **Access to Installation During Force Protection Conditions (FPCONS)**

The Contractor will be assigned a mission essential designation IAW requirements contained in Scott Air Force Base (SAFB) Integrated Defense Plan 31-101. Only the installation commander or the unit commander will designate mission essential reporting.

5.10.9 **Mission Essential Personnel**

The Government has identified a portion of the Contractor services performed under this contract as essential Contractor support of mission essential functions. The services identified as Mission Essential Contractor Services are inclusive to Task 5: Operations Support.

The Contractor shall ensure personnel required to accomplish tasks designated as Mission Essential report to duty stations under all circumstances to achieve DoD missions.

The Contractor shall provide a list of essential personnel required to perform the tasks to CO and COR no later than 10 business days after contract award. This list will be maintained by the Contractor with updates provided to the CO and COR with any personnel changes or as

required. The PMO will be responsible for providing Government security personnel with the list of Mission Essential Contractor personnel to enable access to Government facilities when non-essential personnel are barred. Contractor shall operate IAW DFAR 252.237-7023 Continuation of Essential Contractor Services.

Mission Essential Personnel are personnel allowed to enter Scott AFB during periods of restricted access as designated by the Wing Commander. Contractor personnel may be required to relocate to alternate locations within the CONUS or OCONUS in the events of a critical occurrence. The Contractor shall be required to participate in disaster, emergency preparedness, and Continuity of Operations (COOP)/Failover exercises.

5.10.10 **Site Security**

A GDSS Program node shall be assigned, and the Contractor shall comply with internal security. All Contractor personnel shall be briefed on site security operating procedures prior to or 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.

5.10.11 **Property Protection**

Property protection for the facility where the 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 DAFI 31-101, Integrated Defense, and command/local directives.

The Contractor shall be responsible for safeguarding all government equipment, information, and property provided for Contractor use. At the close of each work period, government facilities, equipment, and materials will be secured. The Contractor shall meet Air Force standards for storing, processing, and handling classified information and systems. Additionally, all resources (e.g. maps, publication/instructions, photos) provided by the Government to assist the Contractor in the performance of their contract will be surrendered upon termination of employment or the end of the contract performance period.

5.11 **Government Property**

Government-furnished property means property in the possession of, or directly acquired by, the Government and subsequently furnished to the contractor for performance of a contract. Government-furnished property includes, but is not limited to, spares and property furnished for repair, maintenance, overhaul, or modification. Government-furnished property also incudes contractor-acquired property if the contractor-acquired property is a deliverable under a cost contract when accepted by the Government for continued use under the contract.

Government property that is incidental to the place of performance, when the contract requires contractor personnel to be located on a Government site or installation, and when the property used by the contractor within the location, remains accountable to the Government. Items considered to be incidental to the place of performance include, for example, office space, desks, chairs, telephones, computers, and fax machines.

5.11.1 **Government Furnished Property/Equipment/Material/Information (GFP/GFE/GFM/GFI)**

The Government will provide a list of GFP/GFE/GFM. GFI, i.e., software code and associated documentation will be provided by the PM. The Contractor shall identify, maintain, and account for all GFP/GFE/GFI, using the Contract Number, Task Order Number, Serial Number and other information as required by the PCO. The Contractor shall assess initial GFP/GFE 30 days

after receipt of delivery. The Contractor shall identify any defects in GFP in sufficient time to allow the Government to correct identified defects and prevent impacts to established testing/integration events for software deliverables. The Contractor shall coordinate with the PCO and the COR for proper disposition of the GFP/GFE/GFM/GFI, if necessary. The Contractor shall maintain and update the GFP/GPE/GFI List to reflect all received items under this contract. The Contractor shall coordinate with the PCO and the COR for proper disposition of the GFP/GFE, if necessary.

5.11.2 Asset Management

The Contractor shall provide asset management for GFP/GFE/GFM/GFI by accomplishing the following per Air Force Manual 33-153 Information Technology (IT) Asset Management or current regulation:

- Maintain and update the GFP/GPE/GFI List to reflect all received items under this contract.
- Provide inventory tracking, planning, maintenance coordination, etc. (CDRL A007).
- Tag all assets and track equipment deployment location and status
- Track the status of equipment warranties and monitor and manage software licenses, including obsolete applications, under- or over-licensed applications and licenses due for renewal.
- Allow Government audits in the Contractor facility as required.

5.11.3 Incidental Equipment and Property

The Government will make available the following as required to support any on-site effort: office supplies, office space, office equipment (e.g. computers), and network access, Government and Contractor documentation, access to facilities and systems. All materials shall remain the property of the Government and the Contractor shall return them to the Government upon request or at the end of the contract period of performance. Any equipment such as laptops or phones provided to Contractor personnel by the Government shall be returned at the termination of the engagement or at another time mutually agreeable to both parties.

5.12 Contractor Personnel

5.12.1 Health and Safety

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, and airfield operations. The Contractor must 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. The COR shall provide copies of publications not available on the web and updates as they become available.

5.12.2 Training and Certification Expenses

The Contractor shall supply and bear all the training cost (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.

The Contractor shall supply and bear all the cost (salary, tuition, course materials, travel, and per diem) for its employee certifications.

5.12.3 **Section 508 of the Rehabilitation Act of 1973 Compliance**

IAW FAR 39.204(a)(1) and 36 CFR Part 1194.3(a) this acquisition is for a national security system and the requirements for acquisitions of Electronic and Information Technology (EIT) supplies and services do not apply to this acquisition.

5.12.4 **Contract Manpower Reporting**

In order to support the requirements of title 10, U.S.C., section 235 and 2330a, DoD Contractors will report ALL Contractor labor hours (including subcontractor labor hours) required for performance of services provided under this contract for AFLCMC, via the Service Contract Reporting (SCR) section of the System for Award Management (SAM) (http://sam.gov). 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. A DoD guidebook for Service contract Reporting in the SAM is available at https://dodprocurementtoolbox.com/site-pages/service-contract-reporting-scr. GSA has posted guidance at https://sam.gov, search the "HELP" section. Should Contractors have issues using SAM, contact the Federal Service Desk at https://www.fsd.gov.

5.12.5 **Organizational Conflict of Interest (OCI)**

If during performance of this contract there is an actual or perceived OCI by the contractor, its employees, or subcontractors, the Contractor shall notify the CO immediately and submit an Organizational Conflict of Interest Identification and Mitigation Plan (OIMP) to the COR and CO at the request of the CO. The government accepted OIMP shall be incorporated by reference into the contract. If applicable 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.

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

APPENDIX A

Non-Disclosure Agreement

I understand that, in the course of my support of the CONTRACTOR Team to the Air Force Life Cycle Management Center (AFLCMC/HBM) under the Global Decision Support Systems (GDSS) Application, Implementation, Modernization and Support (AIMS), I may be exposed to Sensitive Information, which may be provided to, or generated by, the Government or other Contractors which may be proprietary, confidential, or otherwise sensitive to various Contractors and their suppliers. For purposes of this Non-Disclosure Agreement (NDA), the terms Sensitive Information are as defined:

- **Sensitive Government Information (SGI).** Information that may be exempt from mandatory release to the public under the Freedom of Information Act (FOIA) and that can be marked "For Official Use Only (FOUO)" or "Controlled Unclassified Information (CUI)". It includes Source Selection Information, as that term is defined in FAR 2.101, Definitions, and any analyses or other work submitted to the Government under this contract when designated as such by the Contracting Officer.
- **Sensitive Program Information (SPI).** Sensitive Program Information includes one of the three types of information: 3rd Party Contractor Proprietary Information, Government Proprietary Information or Source Selection Information. One objective of the GDSS AIMS OCI Mitigation Plan is to protect these types of information from unauthorized disclosure.

Accordingly, I agree not to disclose outside of the AFLCMC/HBM Government organization of which I am a part and the associated AFLCMC/HBM support staff, unless necessary for performance of GDSS AIMS, any Sensitive Information unless otherwise authorized in writing by the cognizant Government Contracting Officer. However, as part of the GDSS AIMS contract, CONTRACTOR is required to interact with other development Contractors in order to complete GDSS AIMS mission requirements, and this NDA allows for those specific interactions. I further agree to discharge any contract related duties with complete impartiality and objectivity.

I agree to use and examine Sensitive Information exclusively in the performance of work required to carry out my duties under GDSS AIMS which I support and agree to take suitable steps to prevent the disclosure of such information to any party other than those authorized by the cognizant Government Contracting Officer. At the conclusion of my performance on this contract, or upon the request of AFLCMC/HBM, I agree to surrender all contract information, notes, records, or data of any nature gathered or generated during my assignment. I will have no ownership or right to possess such data and information except to fulfill specific AFLCMC/HBM GDSS AIMS work assignments. The rights and obligations of the parties to this Agreement shall not be assignable or used to benefit third parties.

I further agree that I will report to the CONTRACTOR Contracts Manager and Program Manager any known or suspected violations of the procedures established for the protection of Sensitive Information and any circumstances indicating that the advice, assistance, and performance rendered by CONTRACTOR and its teammates to AFLCMC/HBM under GDSS AIMS is anything less than impartial and objective.

I, the undersigned, hereby certify that I fully understand the above Agreement and agree to abide by the provisions, restrictions and prohibitions of this Agreement.

(Printed Name) (Signature) (Date)

ATTACHMENT 1 – Sample: What's New Document

GDSS Version X.X.X. 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. *Insert a screen capture of the menu option with an output of the display that includes the new mission planner feature.* *Hyperlink: For additional information on how to use the Map click here.*
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. *Insert a screen capture of the password reset popup window.* *Hyperlink: For additional information on Accounts click here.*
New Crew Scheduling Capabilities	
	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. Provide instructions for how to disable the default filter; insert screen captures to visually assist the user in walking through the process of changing and saving their settings. *Hyperlink: For additional information on how to schedule crew members click here.*

ATTACHMENT 2 – Sample Software Problem Report (SPR) and Baseline Change Report (BCR)

SPRs and BCRs will all have the following features for control purposes:

- IDENTIFICATION. Control number, date submitted, system identification (title, version, and environment), point of contact (name, office, contact information).
- DESCRIPTION. (See example below) Short title, description of change, source documentation; severity, classification, priority; justification, functional impact, workaround, attachments.
- ANALYSIS. Cost estimates by functional analyst, data system analyst, developer; program analysis, name of analyst, recommended action; targeted release version.
- APPROVAL. Functional manager comments; checks for requirements manager, configuration management, test manager.
- 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 that 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 ASCI 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 ASCI 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