	GLOBAL DECISION SUPPORT SYSTEM (GDSS) COMMAND & CONTROL SYSTEMS SERVICES (C2SS)
Organization:	**HQ AMC C2 SYSTEMS BRANCH (HQ AMC/A6IM)**
Address:	**203 W Losey St, Scott AFB, IL 62225**

Performance Work Statement

1. Description of Services

1.1 Background

The Global Decision Support System (GDSS) is maintained/sustained by the United States Air Force (USAF), Headquarters (HQ) Air Mobility Command (AMC). In 2011, GDSS replaced multiple legacy systems with a single enhanced system; a modernized, fully integrated and enhanced Command and Control (C2) decision support system using open systems infrastructure and a shared relational database. GDSS supports the Defense Transportation System and Distribution Process Owner migration strategies. GDSS is designed around a client-server environment composed of web applications, server processes, Commercial Off-the-Shelf (COTS) relational database management system, database schema, and supporting utility scripts. The COTS supporting the current design include UNIX, Oracle, and Microsoft products. GDSS is deployed on the US Transportation Command (USTRANSCOM) Distributed Enclave (DE) in a multi-master replicated fail-over environment on host infrastructures maintained by the Government. General network operations and maintenance is handled by the Government, to include local network updates/patches as part of their security policies. GDSS Object Processor (GOP)/Mobility Enterprise Information Service (MEIS3) GDSS Object Processor (MGOP) is migrating to the GDSS Mobility Communication Services (MCS). Support will continue to be required for MGOP and MEIS v3.3.3.

As the Mobility Air Forces (MAF's) principal C2 system, GDSS is the execution authority for mission management, providing robust capabilities in a net-centric environment, and allowing access and information sharing across unclassified and classified domains using continuous multi-master replicated databases. GDSS interoperates with Air Force, Army, and Joint C2 systems, and interfaces with other key Department of Defense (DOD), USTRANSCOM, Joint and AMC C2 and transportation management systems while utilizing the USTRANSCOM Distributed Enclave architecture. GDSS is an extension of the USTRANSCOM network providing a full computing infrastructure to include network, servers, security and storage. Replication is provided using four near real-time replicated unclassified and classified C2 enclaves for redundancy and performance. Currently, there are over 20,000 active user accounts from 261 major sites world-wide. GDSS user demographics include aircrew, airfield managers, C2 controllers, flight managers, intelligence, maintenance, mission planners, stage managers, transportation managers, and weather. GDSS directly draws and/or pushes data to the following systems: Advanced Computer Flight Planning System, Virtual Threat Assessor, Single Mobility System, USTRANSCOM Reference Data Management, AF Aircraft Maintenance System-GO81, Aviation Resource Management System, 618 Air Operations Center (AOC) Data and Web Services, Weather Data Analysis system, Air National Guard, Cargo Movement Operations System, DEAMS Consolidated Billing System, 15/17 Operational Weather Squadron, and Global Combat Support System; and also interfaces with 18 additional systems through MEIS3.

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

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

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

Dynamic Mission Re-Planning (DMR) is a transportation initiative designed to enhance AMC's ability to re-plan missions in execution by providing a capability to recognize and react to a potential problem or event, to automatically assess the significance of the event, recognize down line or associated mission impacts, and present the decision maker with weighted options. DMR consists of a family of work center focused applications that provide 618th Air Operations Center Tanker Airlift Control Center (618 AOC TACC) users an effective way of visualizing the myriad of factors that could result in a delay or deviation of a planned mission.

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

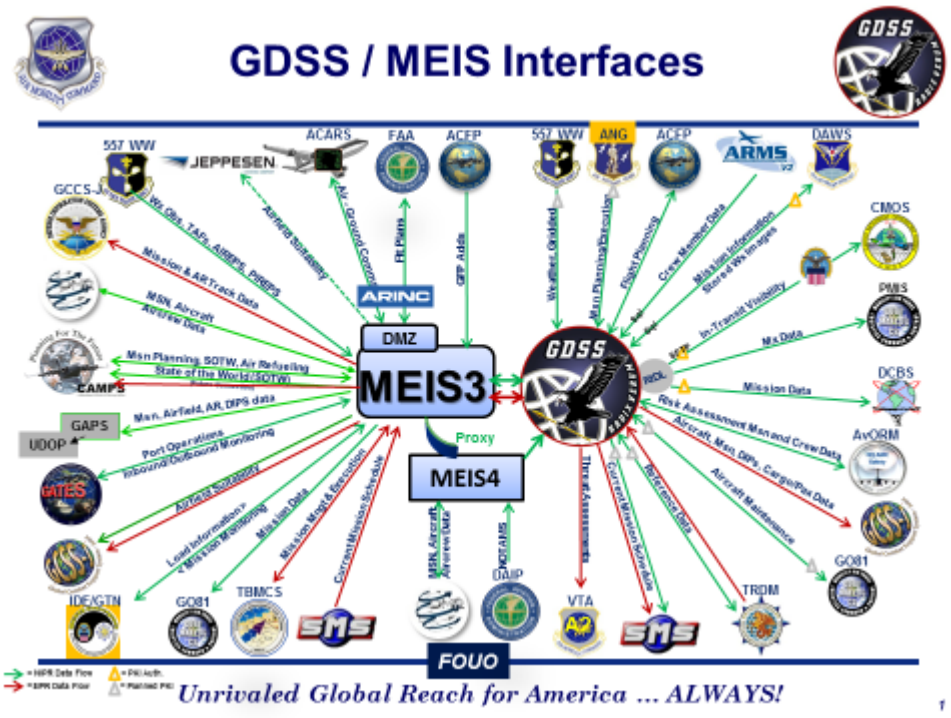
1.2 Mission and Organization

AMC/A6's mission is to provide integrated Command, Control, Communications, and Computer Information (C4I) systems and manage strategic C4I resources in support of AMC's 618th AOC) – Tactical Airlift Control Center (TACC) global air mobility mission. HQ AMC/A6IM requires 24x7 Command and Control Systems Services (C2SS) for users of the classified and unclassified GDSS. The Contractor shall provide C2SS services for USTRANSCOM's GDSS program managed by HQ AMC/A6IM. The GDSS Program of Record includes the following applications: GDSS, AvORM, EMC, MEIS 3.3.3, MGOP, MCS, MSD, GDSS Training Suites, GDSS Exercise Suites, Prototype Suites and DMR. Within this document these applications will be referred to as GDSS unless otherwise stated. The GDSS user community consists of approximately 20,000 users located throughout the world.

At the highest level, GDSS users are mission operators from the military services, DOD, and other Federal agencies. The capabilities required in the Command and Control of the MAF include: Deployment and Distribution, Understand, Planning, Decide, Direct, and Execute. GDSS ties together these capabilities with the warfighter.

The following diagram (Fig. 1-1) illustrates the current interfaces that give GDSS a formidable and dynamic command and control capability; Situational awareness from strategic to finite details; Ability to direct or re-direct forces with accuracy, current data, integration with Air Traffic Control (ATC), weather, and in real or near real time.

The Contractor shall be required to understand these system relationships during the transition period (30 days after contract award); the nature of each interface in terms of the data it pulls, pushes or gets from and/or to GDSS and the purpose of that data, as well as a comprehensive technical understanding of each interface connected to GDSS. Figure 1-1 is for informational purposes only and subject to change as interfaces are modified.



2. Scope

GDSS requires 24x7x365 C2SS for users of the classified and unclassified network. The contractor shall provide C2SS for USTRANSCOM's GDSS program managed by HQ AMC/A6IM. The contractor shall provide the following C2SS for classified and unclassified GDSS users:

- Functional subject matter expertise for end users with assistance on GDSS application functionality, C2 operational issues related to user inputs to and outputs from GDSS, and related user productivity (e.g., reduce user actions/inputs to complete a task).
- System/application and database access account management services for GDSS and MEIS.
- Operational validation for GDSS using GDSS user manual, release fielding plan, and approved test.
- End user assistance on C2 issues in support of HQ AMC participation in the Chairman's Exercise Program (CEP), Joint Exercise Program (JEP) and Joint National Training Capability (JNTC) exercises. Local exercises and interface testing between AMC and other MAJCOMs.
- 24x7x365 support to end-users with assistance on program specific applications functionality, operational issues related to user inputs to and outputs from the program applications, and productivity help;
- Customized troubleshooting and resolution;
- Subject matter expertise to support Government interactions, meetings, planning and account management;
- Sustainment services, for example, Corrective, Adaptive, Enhancement, or Perfective Maintenance (IEEE Std 1219);
- GDSS system releases in a non-service interrupted process;
- Support to fielding and operational maintenance;
- Implement agile development activities and administrative support to meet financial and programmatic reporting needs

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

USTRANSCOM TCJ6 Memo to TCJ3C (Mission Area Manager), Subject: CIO Guidance for FY19 Budget Estimate Submission (BES) letter dated, 19 July 2016.

This includes Data Center Migration; compliance with DITPR, E-Gov/FISMA, Cyber Scoreboard; PoR CCE Migration: Common Development Environment (CDE) 3.0; DOD Risk Management Framework (RMF) Implementation; Technology Strategy Management; Service Oriented Architecture, EI Portfolio Initiatives, and Mobile Service Device (MSD).

3. Requirements/Description of Services

The Contractor shall provide GDSS C2SS 24x7x365. Support applications include: MAF C2, Mission Planning and Air Refueling, Aircraft Management and Logistics, AvORM, Mission Management and Execution, Sequence of Events, Flight Management, Flight Planning, Crew Management, Location Management, Air Tasking Order Integration, Weather, Diplomatic Clearance Management and Exercise Management Console and DMR.

Except for those items specifically stated as Government-furnished, the Contractor shall furnish everything needed to perform this contract. The Contractor shall perform the following tasks:

- Task 1 – 24x7x365 GDSS C2SS
- Task 2 – GDSS Account Management Services
- Task 3 – GDSS Operational Validation Services
- Task 4 – Program Management

3.1 Task 1 – GDSS C2SS Operations

3.1.1 Sub Task 1 – 24x7x365 GDSS C2SS – Primary Location

The contractor shall provide the following Level II functions:

- Provide onsite C2SS services 24x7x365 at government provided facilities
    - Contractor personnel providing situational technical support will be required to support three-shift functions to support mission requirements

- Assist users with understanding the system and procedures necessary to accomplish the user's tasks.
- Supply C2 Systems services for the continuous operation of the fixed and deployed systems for approved users in or supporting Active, Guard, and Reserve units.
- When trouble calls come in, enter trouble ticket calls into Remedy a Government-provided electronic log, Computer Software Trouble Reporting System; include user information such as trouble ticket number, date and time received, corrective action, date and time resolved, user name, and date and time notified. Interface and coordinate Remedy trouble tickets with appropriate points of contact to resolve problems or issues.
- Update and maintain C2SS procedures relative to this effort.
- Ensure the most current information on the functional operation is available.
- Participate in problem resolution and propose software problem reports for program review.
- Assist users in documenting requested software changes, using the Government Change Request process.
- Track Remedy tickets and monitor them daily until closure. Provide GDSS PMO with weekly ticket report.(A009)
- Maintain and follow procedures and methods to obtain resolution within 60 minutes from call for at least 90% of trouble calls.
- Provide Client Support Administrator (CSA) assistance in accordance with AFI33-115v1 in support of C2 Systems Services equipment.

- Provide functional expertise with regard to information services provided by the MEIS and DRM. This shall be accomplished by reviewing data in GDSS or providing information to other support personnel to facilitate troubleshooting or reported data flow issues.
- Provide functional expertise ensuring the changing regulations and interfaces (such as civil aviation, military aviation, and diplomatic clearances) are being addressed within the GDSS user community and within the system itself.
- Manage and maintain user DD Form 2875s.
- Provide functional expertise with regard to the Mission Timeline (MTL) application. Ensure the MTL web application allows users to view mission events along a timeline, and in the "What If" mode so users can explore the impact that changes to the mission will have on the mission and its resources. This will include information about mission resources such as aircraft, aircrew, airfield, and cargo including visual cues that indicate events, violations, restrictions, warnings, cautions, and notes relating to the use of these resources.
- Provide functional expertise with regard to the Resource Finder (RF) application and ensure the application's tooltips and windows can provide additional information about the mission and mission resources when required. The MTL application shall link directly to the RF application, allowing users to find mission resources. The RF web application should allow users to search for AMC suitable airfield resources within a selected geographical area and to view selected airfield details. The RF will include searches for available aircraft resources filtered by geographic area, Mission Design Series (MDS), mission type, and mission priority. Note that this application incorporates training and unassigned filters as well as view of selected aircraft details. Aircraft details and resource information typically include mission number, location, destination, MDS and tail number.
- Maintain phone roster (A002) to be used as an emergency notification contact/escalation list of all Contractor employees for this effort.
- Support the USTRANSCOM directed GDSS migration to a commercial Cloud environment and utilize a DevOps paradigm. For Cloud Integration, C2SS will provide functional expertise to support the integration into the Cloud.

3.1.2 Sub Task 2 – 618th Air Operations Center (618 AOC) – Tactical Airlift Control Center (TACC) 24x7 Over-the-Shoulder Services

Services shall be the same as Sub Task 1; however, the Contractor shall provide over-the-shoulder support to TACC personnel, Building 1600, to resolve problems.

3.2 Task 2 – GDSS Account Management Services

These services shall be provided for operational, exercise, and training requirements IAW Government manuals and instructions referenced herein and GDSS Account Management Documents.

- Create User Accounts
- Set User Authorizations
- Identify Inactive Accounts
- Remove Inactive Accounts
- Update Account Management Application
- Provide Account Usage and Security Services
- Validate the status of user accounts in coordination with the supported systems
- Manage and perform account validation process to support the Risk Management Framework (RMF) process
- Maintain the Unit Program Account Manager (UPAM) appointment letters and add/remove privileges as appropriate
- Provide account management services for GDSS and MEIS
- Maintain GDSS component permissions (roles and privileges) for users
- Provide on-site account management services 24x7x365 at Government-provided facilities
- Create/update/deliver account management checklist as requested by GDSS PMO

- Validate accounts IAW Government directives and approved procedures
- Support the USTRANSCOM directed GDSS migration to a commercial Cloud environment and utilize a DevOps paradigm. For Cloud Integration, C2SS will provide functional expertise to support the integration into the Cloud.

3.3 Task 3 – GDSS Operational Validation Services

The Contractor shall accomplish the following:

- Prepare and submit Validation Plan (A003) as defined in the GDSS release fielding plan which will be provided by the Government with each release
- Conduct validation in coordination with the GDSS PMO
- Prepare and submit validation report (A004)
- Support the USTRANSCOM directed GDSS migration to a commercial Cloud environment and utilize a DevOps paradigm. For Cloud Integration, C2SS will provide functional expertise to support the integration into the Cloud.

3.4 Task 4 – Program Management

The Contractor shall provide the planning, direction, coordination, and control necessary for effective and efficient accomplishment of all requirements contained in this PWS. The Contractor's Project Manager shall coordinate work carried out under this PWS with the appropriate Contracting Officer's Representative (COR). The Contractor shall meet stated Government requirements and milestones and must advise the COR as soon as possible whenever requirements and milestones cannot be met. Actual or projected failure to meet PWS requirements and milestones shall be orally reported to the COR as soon as the information is available and also in the appropriate periodic reports, test reports, and review minutes. Support the USTRANSCOM directed GDSS migrate to a commercial Cloud environment and to utilize a DevOps paradigm. For Cloud Integration, the contractor will utilize USTRANSCOMs DevOps model (tools, methods and processes) as directed, if needed. Any deviation from DevOps model must be approved by the USTRANSCOM TCJ6 Enterprise Change Control Board (CCB). The developer is required to provide all software assets required to build, deploy, test, operationalize and run an application.

3.4.1 Sub Task 1 – Contractor Progress and Monthly Status Report (MSR)

The Contractor shall provide MSR (A005) of Contractor progress, status, and management activity to the COR.

3.4.2 Sub Task 2 – Meetings and Minutes

The Contractor shall notify the COR of any meetings they will attend which pertain to this effort, not specifically convened by the COR or members of the GDSS PMO. At the conclusion of each meeting, the contractor shall provide meeting minutes to the COR.

3.4.3 Sub Task 3 – Management Plan

The contractor shall submit a Management Plan (A001) which succinctly describes the approach the contractor will use to perform all PWS tasks and other contract requirements.

3.4.4 Sub Task 4 – Quality Control

The contractor shall provide a Quality Control Program documented in a Quality Control Plan (A010). Establish and maintain a quality control program and document in a Quality Control Plan (QCP) approved in writing by the COR. In establishing and maintaining a Quality Control Program, the contractor shall plan, develop and implement

procedures and practices to ensure that all requirements of the contract are complied with fully. The COR will audit all processes outlined in the QCP. The QCP shall also include a non-compliance reporting and tracking process.

4. Deliverables Management

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

All deliverables are listed as DD Form 1423s Contract Data Requirements List and are reflected in the table below. All deliverables shall be in accordance with the instructions on the DD Form 1423. Deliverables, once submitted, cannot be revised but can be appended. All documentation generated becomes Government property.

Contract Data Requirements List (CDRL) Number	Deliverable Title	PWS Para
A001	Management Plan	3.4.3
A002	Phone Roster	3.1.1
A003	Validation Plan	3.3
A004	Validation Report	3.3, 8.4.2
A005	Monthly Status Report (MSR)	3.4.1
A006	Meeting Minutes	3.4.2
A007	Equipment Inventory Report (EIR)	6.3
A008	Transition Plan, Phase-In/Phase-Out	15
A009	Ticket Report.	3.1.1
A010	Quality Control Plan	3.4.4

5. Services Summary (SS)

The SS table below summarizes the most important performance objectives and performance thresholds (specific standards) as identified within the body of the PWS. The absence of any performance objective and threshold from this SS shall not detract from its enforceability nor limit the rights or remedies of the Government under any provision of the contract. Metrics shall be calculated quarterly. The SS will be in accordance with AFI 63-101,

Acquisition and Sustainment Life Cycle Management, AFI 10-601, Capabilities-Based Requirements Development and Federal Acquisition Regulation (FAR) Subpart 37.6, Performance-Based Acquisition.

5.1 Table 1 – Specific Standards

Performance objective	PWS Para	Performance Threshold	
Input electronic log of trouble calls into Remedy	3.1.1	Enter trouble ticket calls into the Government-provided electronic log, Computer Software Trouble Reporting System (Remedy), accurately at least 95% of the time. Trouble tickets submitted into Remedy within 15 minutes of the calls.	
Provide trouble ticket resolution	3.1.1	Resolution of customer problem within 60 minutes from call for at least 90% of trouble calls.	
Provide Account Management Services	3.2	Account privileges provided or restored within 60 minutes of request, at least 90% of the time. Accounts validated nightly with no more than 5% inactive users being carried as active at any given time.	
Provide Validation Plan	3.3, 8.4.2	Provided to the Government with each release.	
Provide Validation Report	3.3, 8.4.2	Due verbally/email within 1 work day of test completion and 99% accurate. Written report due five work days after the test event schedule as defined in the GDSS fielding plan.	
Provide Program Management Services	3.4	Accurate reports, minutes, and briefings provided by the scheduled due date at least 95% of the time. Information provided to be at least 95% accurate. All inaccuracies corrected within one work day.	

6. Government Property

The Government will provide property for the Contractor to use in the performance of the contract. The Contractor shall account for and maintain all the Government-provided materials, property, and equipment in accordance with the Government Property clause included in the contract.

6.1 Incidental Equipment & 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 will 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. If the Contractor is off-site, the Government will provide computers, virtual private network (VPN) hardware, and a copy of any appropriate software, as well as existing scripts and any script-creation tools. The Government will provide the following computer software:

- GDSS client application
- Remedy client
- Air Force Standard Desktop applications
- Monitoring software

6.2 Government Furnished Information (GFI)

The Government will provide GDSS documentation to include user manuals, test plans, and architectures. Reference Appendix A for applicable regulations, instructions, and policy letters.

6.3 Equipment Inventory Record (EIR)

The Contractor shall prepare and maintain an equipment inventory record (A007). Additionally, report to the COR via marked-up inventory report any discrepancies between the list of Government property provided and the actual inventory.

6.4 Contractor-Furnished Items and Services

Except for those items or services specifically stated in Section 5 as Government-furnished, the Contractor shall furnish everything needed to perform this contract.

7. General Information

7.1 Points of Contact

Contractor's Project Manager – the Contractor shall provide the name of a Contractor Project Manager who shall be responsible for the performance of the work. The name of the Contractor Project Manager and alternate(s), who shall act for the Contractor when the Contractor Project Manager is absent, shall be designated in writing to the Contracting Officer (CO) prior to the commencement of the period of performance. The Contractor shall notify the CO in writing of any changes to personnel within three workdays after information is known.

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

7.3 Period of Performance (POP)

The planned POP includes a 30 day phase-in period followed by a 12-month base period, three 12-month option periods, one 11-month option period, plus an option for a 6-month Extension of Services.

7.4 Place of Performance

HQ AMC/A6IM shall provide limited work space for up to eight C2SS personnel per shift and their related tasks on Scott AFB. Any remaining staff will need to reside at a Contractor facility located within Scott AFB commuting distance (50-mile radius). All meetings, reviews, and audits will be held at Scott AFB or the local Contractor's facilities, except when alternate locations are agreed upon by the Contractor and the COR. Management, technical studies, analysis, and associated activities may be conducted at the most feasible and economical location.

7.5 Duty Hours

C2SS shall be operational 24x7x365, federal holidays included. Federal holidays are defined as the dates the following holidays are observed: New Year's Day, Martin Luther King's Birthday, President's Day, Memorial Day, Independence Day, Labor Day, Columbus Day, Veteran's Day, Thanksgiving Day, Christmas Day, other federal holidays declared by Congress or the President, and base closures, to include closures due to inclement weather. There may be occasions when support contractors are invited to participate in morale and recreational activities (i.e., holiday parties, golf outings, sport days and other various social events). Contractor employees shall not be directed to attend such events by the Government. Since a contract employee is not a government employee, the employee cannot be granted the same duty time activities as Government employees. Participation in such events should be in accordance with the company's policies and compensation system.

7.6 Travel

Travel for performance of this PWS is not anticipated. However, if at any time travel is required, a Contract modification will be negotiated and executed by the Contracting Officer.

8. Security

8.1 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 a LEADS check will be denied access to the installation. Information required to conduct a LEADS check includes: full name, driver's license number, and/or social security number, date of birth of the person entering the installation, and completion of a background check questionnaire. The Contractor must have this information ready to provide to the installation's Visitor Control Center, if requested.

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

8.2 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 will comply with DODI 5220.22-M, DOD 5220.22-R, and DOD 5200.01-M V1-4. Facility and employee security clearances are obtained according to DOD 5220.22M. Contractor must have a facility clearance, as required by DD Form 254, prior to award of contract. 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.

8.2.1 After hours Security Checks

Contractors may be required to conduct facilities security checks.

8.2.2 Privacy Information

Work on this project may require personnel to 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.

8.2.3 DD Form 254 Requirements

The contractor shall comply with all appropriate provisions of the security regulations. Specific security requirements are identified in the DD Form 254, Department of Defense Contract Security Classification Specification.

8.3 Personnel Security

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

The Contractor must provide all personnel necessary to perform required services, as defined in this PWS. All services provided must be consistent with Air Force policy, rules, regulations, instructions, orders, guidance and practices.

8.3.1 Protection of System Data

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

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

8.3.1.1 Non-Disclosure Agreements

To safeguard information, the contractor must enter into non-disclosure agreements with the responsible local security manager.

8.3.2 Access to Government Systems and to Installation during Force Protection Conditions (FPCONs)

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. Contractor personnel shall comply with all AMC security requirements pursuant to DOD 5200.2, DOD Personnel Security Program, which requires DOD military, and civilian personnel, as well as DOD consultant and Contractor personnel who perform work on sensitive AIS to be assigned to positions which are designated sensitive. All personnel must complete Annual Information Assurance training via online CBT (https://amc.csd.disa.mil/). All personnel must comply with DOD 8570.01-M, Information Assurance Workforce Improvement Program and must provide certifications prior to contract start date. Contractor employees assigned to performing functional services duties, which include Account Management and System Administration shall meet and maintain DOD 8570.01-M certification Information Assurance Technical (IAT) Level I, A+ certification or Government-approved equivalent by full performance start date. Contractor employees assigned to performing CSA duties, and any contract lead shall meet and maintain DOD 8570.01-M certification IAT Level II certification by full performance start date.

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

Contractor will be assigned a mission essential designation IAW requirements contained in the installation's Integrated Defense Plan or Installation Antiterrorism Plan. Only the installation commander or the unit commander requesting contract services will assign mission essential designation.

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

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

8.3.2.1 Mission Essential Personnel

Certain personnel providing services under this contract will be designated as Mission Essential Personnel. Contractor shall ensure personnel required to accomplish tasks designated as Mission Essential Personnel report to assigned work locations and perform required tasks, regardless of weather or security conditions. The Government has identified Task 1: 24x7x365 GDSS C2SS level II functions; Task 2: GDSS Account Management Services and Task 3: GDSS Operational Validation Services as Mission Essential. 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 start. This list will be maintained by the contractor with updates provided to the CO and COR with any personnel changes or as required. The CO and/or COR will be responsible for providing Government security personnel with list of contractor Mission Essential Personnel to enable access to Government facilities when non-essential personnel are barred. Contractor shall operate IAW DFARS 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 Base 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.

8.3.3 Access to Government Facilities

The Government, based on assessment of the Contractor's need, shall provide the Contractor access to GDSS program facilities from the commencement of the contract until contract completion. Only Contractor (or subcontractor) personnel possessing the proper clearance will be authorized entry to restricted areas. All Contractor

personnel must either have the appropriate building access permissions and ID cards or otherwise must be continuously escorted by Government approved personnel.

8.3.3.1 Property Protection

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

8.3.3.2 Contractor Working in Controlled or Restricted Area

In the event that a Contractor requires access to the controlled or restricted area and does not have the proper security clearance, government will ensure escort(s) are provided to Contractor at all times when within a controlled or restricted area. Based on AMC procedures, Contractors may act as escort officials under certain circumstances. Contractor must have an issued AF Form 1199 and work on base a minimum of four days a week (must have an assigned workspace on base). Contractor is only allowed to escort visitors from the same company for which he/she works, and all visits must for official business. In addition, the Contractor must fulfill, maintain, and comply with all security requirements IAW Integrated Defense and command/local directives. Contractor must comply with security regulations imposed by the installation commander and/or the agency responsible for the project location. Due to specific mission requirements inherent in the nature of controlled or restricted areas on Air Force installations, Government may direct Contractor to leave the controlled or restricted area at any given time.

8.3.3.3 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 on the installation, the Government may direct the Contractor to leave the controlled or restricted areas at any given time. If this direction increases the cost of or the time required to complete the work, the contract price or schedule, or both must be adjusted accordingly through a modification to the contract.

8.3.3.4 Access to Government Facilities with Controlled or Restricted Areas for Replacement Contractor

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

8.4 System Engineering

8.4.1 US Air Force Standard Desktop Configuration (SDC)

All services provided under this contract shall function under the fielded Standard Desktop Configurations (SDCs) and be in compliance with AFI 33-115 (update in draft), i.e. not altering the Air Force SDC.

8.4.2 Operational Validation

The contractor shall conduct operational validation ranging from data entry and display at the user level on the operational system prior to user transition of a new version. The contractor shall accomplish operational validation IAW the Government-approved test plan as specified in the contract. The plan shall consist of a program of tests, inspections and demonstrations to verify compliance with the requirements of this contract. The contractor shall document test results in the test report(s). The contractor shall be responsible for documenting deficiencies in

Remedy. The Validation Report (A004) is due verbally within one work day of test completion. Written report is due five work days after the test event schedule as defined in the GDSS fielding plan.

9. Organizational Conflict of Interest (OCI)

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

9.1 Identification and Mitigation Plan

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

9.2 Mitigation Plan Revision

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

9.3 Violation Reporting

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

10. Non-Personal Services and/or Inherently Governmental Services

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

11. Contractor Identification

11.1 Identification Badges

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

11.2 Identification in the Workplace

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.

11.3 Records, Files, and Documents

All physical records, files, documents, and work papers, provided and/or generated by the Government and/or generated for the Government in performance of this PWS, maintained by the Contractor which are to be transferred or released to the Government or successor Contractor, shall become and remain Government property, including all intellectual property rights, and shall be maintained and disposed of IAW AFMAN 33-363, *Management of Records*; AFI 33-364, *Records Disposition – Procedures and Responsibilities*; the Federal Acquisition Regulation, and/or the Defense Federal Acquisition Regulation Supplement, as applicable.

12. Training

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

12.1 Technical Currency

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

12.2 Certification Cost

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

13. Section 508 Accessibility Standards / Section 508 of the Rehabilitation Act

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

14. Network, Computer, and Information Security

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

14.1 For Official Use Only (FOUO)

Agency information marked "FOR OFFICIAL USE ONLY" or bearing other sensitivity markings shall be handled in accordance with agency information security program regulations and instructions provided on the DD Form 254. This information shall not be divulged or disclosed without agency permission. Requests for disclosure shall be

addresses to Government. Contractor personnel shall ensure information that is considered sensitive or proprietary is not comprised.

14.2 Privacy Act

Work on this project requires that personnel have access to Privacy Information (PII). PII shall be safeguarded in compliance with Federal/DOD PII guidelines, Title 5 U.S.C 552a "The Privacy Act of 1974", DOD Publication 5400.11-R "Department of Defense Privacy Program", and DOD Directive 5400.11 "DOD Privacy Program".

14.3 Safety Requirements

The Contractor shall comply with the latest applicable Federal, State, Air Force, AMC, and Installation, regulations, instructions, policies, management plans and requirements regarding personnel health, occupational and operational safety. The Contractor shall comply with all safety provisions, e.g., technical specifications, technical publications, and federal Occupational Safety and Health Administration (OSHA) standards (Title 29 CFR Part 1910). If there is no applicable OSHA standard, the Contractor shall use other applicable nationally or locally recognized sources of safety, health, and fire prevention standards. The COR shall provide copies of publications not available on the web and updates as they become available.

15. Transition

The transition plan applies only if the contract awardee is not the same as the incumbent contractor.

15.1 Phase-In

A phase-in CLIN will be included in the contract for the phase-in period. A 30 calendar day phase-in period will be available for the new Contractor to assume full responsibility for PWS performance at the end of the phase-in period. Full contract performance must begin immediately following the end of the phase-in period. The Contractor shall provide a Phase-In Plan (A008) including strategy and method of assuming responsibility for tasks described in the PWS and strategy for acquiring qualified, cleared personnel seven calendar days after award. Recurring status briefings will be provided to the COR throughout the phase-in period.

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

- Immediately upon contract start, implement the proposed methods, processes, procedures, and tools as described in the approved phase-in plan
- Within 24 hours of contract start, notify the COR with the names and phone numbers of the Contractor's program manager and task lead
- Within five work days of contract start have key staff in place in order to begin shadowing the incumbent Contractor
- Immediately following the end of the phase-in period, assume full PWS services responsibilities

15.2 Phase-Out

Included in the Transition Plan submitted to the COR, the Contractor shall provide a phase-out strategy (A008) describing the method of transferring responsibility for tasks described in the PWS. Recurring status briefings shall be provided to the COR and associated Contractors throughout the transition period. The Contractor shall cooperate

fully with the COR and any successor Contractor(s) to ensure an orderly transition at the end of this contract. The Contractor shall accomplish the following phase-out tasks:

- Preserve and make available to the COR, if requested, copies of all records and other documentation, developed or acquired under this contract or preceding contracts for this effort, regarding performance of the work required by this contract
- Make available to the COR, upon request, the names, job titles, and duties of all employees who have worked under this contract.
- Permit current employees to be interviewed for possible employment by a successor Contractor
- Provide an orientation for successor Contractor employees
- Supply to the COR, 60 days prior to the completion of the contract
    - Complete backup of all contract and contract related data stored on each employee's hard drive, along with any global data. List of all GFE and COTS utilized in support of this task
    - Soft and hard copies of all procedures and training materials developed as part of this effort
    - Ensure that no contract data is corrupted, changed, or altered such that it would cause damage to the Government
- System documentation is to be compliant with CMMI Level 3 standards. The method of delivery will be by mutual agreement between the GDSS PMO and the Contractor
- Within 30 days of contract completion the Contractor shall, in conjunction with the COR, conduct a joint inventory of the GFE and reconcile to the list EIR
- Upon contract completion, the Contractor shall provide access to all information and data secured by password or key encryption card. All data locked by key card shell be unlocked prior to turn-in or destruction of the card
- The Contractor shall unlock, or provide the keys to any and all equipment physically locked

16. Protecting Government Intellectual Property

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

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

- 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 Sybase 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.

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

17. Contractor Manpower Reporting

The Contractor shall report ALL Contractor labor hours (including subcontractor labor hours) required for performance of services provided under this contract for the GDSS Application Support via a secure data collection site. The Contractor is required to completely fill in all required data fields at http://www.ecmra.mil.

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

Appendix 1: Definitions

TERM	DEFINITION
AMC	Air Mobility Command
AFRC	Air Force Reserve Command
ANG	Air National Guard
C2	Command and Control
CHOP	Change of Operational Control
CLIN	Contract Line Item
CO	Contracting Officer
COR	Contracting Officer Representative
CRAF	Civil Reserve Air Fleet
DDOC	Deployment Distribution Operations Center
DIRMOBFOR	Director of Mobility Forces
DOD	Department of Defense
GATES	Global Air Transportation Execution System
GCCS	Global Command and Control System
GDSS	Global Decision Support System
GFE	Government Furnished Equipment
GFI	Government Furnished Information
JOPES	Joint Operation Planning and Execution System
JTR	Joint Travel Regulations
MSR	Monthly Status Report
NIPRNET	Non-Secure Internet Protocol Router Network
OPSUM	Operations Summary
POC	Point of Contact
PWS	Performance Work Statement
SAAM	Special Assignment Airlift Mission
SIPRNET	Secret Internet Protocol Router Network
SMS	Single Mobility System
STACS	Suspense Tracking Application for Command Staff
TDD	Theater Direct Delivery
TMT	Task Management Tool
USCENTCOM	United States Central Command
USTRANSCOM	United States Transportation Command
XON	618 AOC Mission Support Directorate
XOND	618 AOC (TACC) Data Division
XONT	618 AOC (TACC) Technology Division
XOP	618 AOC (TACC) Global Readiness Directorate

Appendix 2: Non-Disclosure Agreement

Non-Disclosure Agreement for Contractor Employees Supporting AMC Contracts

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

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

1. I, _____ currently an employee of _____, hereby agree to the terms and conditions set forth below:

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

3. In the course of performing under contract/order number _____ or some other contract or subcontract for the AMC I agree to:

    a) Use only for Government purpose any and all confidential business information, Contractor bid or proposal information, and/or source selection sensitive information to which I am given access. I agree not to disclose "nonpublic information" by any means (in whole or in part, alone or in combination with other information, directly or indirectly or derivatively) to any person except to a U.S. Government official with a need to know or to a non-Government person (including, but not limited to, a person in my company, affiliated companies, subcontractors, etc.) who has a need to know related to the immediate contract/order, has executed a valid form of this non-disclosure agreement, and receives prior clearance by the contracting officer. All distribution of the documents will be controlled with the concurrence of the contracting officer.

b) Not use such information for any non-Governmental purposes, including, but not limited to, the preparation of bids or proposals, or the development or execution of other business or commercial ventures.

c) Store the information in such a manner as to prevent inadvertent disclosure or releases to individuals who has not been authorized access to it.

4. I understand that I shall never make an unauthorized disclosure or use of confidential business information, Contractor bid or proposal information, and/or source selection sensitive information unless:

a) The information has otherwise been made available without restriction to the Government, to a competing Contractor, or to the public;

b) The contracting officer determines that such information is not subject to protection from release.

5. I agree that I shall not seek access to "non-public information" beyond what is required for the performance of the services I am contracted to perform. I agree that when I seek access to such information or attend meetings or communicate with other parties about such information, I will identify myself as a Contractor. Should I become aware of any improper or unintentional release or disclosure of "non-public information," I will immediately report it to the contracting officer in writing. I agree that I will return all forms (including copies or reproduction of original documents) of any "non-public information" provided to me by the Government for use in performing my duties to the control of the Government when my duties no longer require this information. By signing below, I certify that I have read and understand the terms of this Non-Disclosure Agreement and voluntarily agree to be bound by its terms.

_____ _____

Signature of Employee/ Date

_____

Printed Employee Name

_____ _____

Signature of Company Official/ Date

_____ _____

Printed Company Official Name

Appendix 3: Government Furnished Equipment (GFE)

The following GFE inventory was conducted XX XXXX XXXX and will be re-accomplished during contract transition. Page X of X of the inventory, not included, is the signature page and does not list GFE.

AIM Inventory needs to be updated……