PERFORMANCE WORK STATEMENT
INSCOM CIO/G6 Enterprise Acquisition

1.0 DESCRIPTION OF SERVICES/INTRODUCTION

The U.S. Army Intelligence and Security Command (INSCOM), a Direct Reporting Unit (DRU) to Headquarters, Department of the Army, G-2, conducts intelligence, security and information operations for military commanders and national decision makers. Charged with providing the war fighter the actionable intelligence needed to understand the battlefield and to focus and leverage combat power, INSCOM collects intelligence information in all intelligence disciplines. INSCOM also conducts a wide range of production activities, ranging from intelligence preparation of the battlefield to situation development, SIGINT analysis, imagery exploitation, and science and technology intelligence production. INSCOM has major responsibilities in the areas of counterintelligence and force protection, electronic warfare, information warfare, and support to force modernization and training. Headquartered at Fort Belvoir, VA INSCOM is a global command with major subordinate commands that tailor their support to the specific needs of different theaters. The command synchronizes the intelligence operations of all INSCOM elements to ensure multi-discipline intelligence support to theater/component warfighters, the Intelligence Community (IC) and other national agencies. INSCOM has 16 subordinate commands and a variety of smaller units with over 16,800 personnel dispersed over 180 locations worldwide.

1.1. Background

1.1.1 Organizational Mission

INSCOM CIO/G6 provides the enabling layer to connect the Army and its tactical formations to defense and national intelligence agencies via NSANET, JWICS, Trojan, and DCGS networks. The ability to provide mission critical intelligence is dependent on the successful operation and maintenance of its Information Technology (IT) worldwide.

1.1.2 CIO/G6 Intent

INSCOM CIO/G6 seeks to provide reliable, uninterrupted availability of Command, Control, Communications, Computers and Information Management (C4IM) including: networks, hardware, software, and specialized tools at the point of customer need.

1.1.3 Environment and Infrastructure Overview

1.1.3.1 Unit Description

The typical INSCOM unit resides in a secure office building with controlled access. Units may have off-site locations the contractor shall support. Employees are located in separate offices or cubicles, supported by networked or stand-alone C4IM Systems (unclassified and at various classification levels). Most facilities contain rooms configured to serve as data and/or communication centers. The working environment typically requires controlled access to

classified information and many of the work locations are within Sensitive Compartmented Information Facilities (SCIF) and in some cases, Special Access Program (SAP) facilities. The equipment supported and technical services provided by this performance work statement (PWS) are used to support worldwide intelligence and C2 operations. The equipment also provides intelligence data to National Command Authorities, members of the Intelligence Community (IC), and various civilian agencies and departments. As used in this PWS, the term C4IM System is defined as the totality of capabilities which are owned, operated, and managed by each site. Included in this definition are the Local Area Networks (LANs) (comprised of copper and/or fiber network media) that reside within the physical spaces controlled by the site and the systems the site takes with them when deployed or travelling in support of other mission requirements. Services provided by the Enterprise (i.e., Department of Defense (DoD), Army, or Intelligence Community (IC)) are not included in this definition and are not the responsibility of the contractor. Note: the contractor is responsible for maintaining the interfaces between the sites' infrastructure and the Enterprise capabilities.

1.1.3.2 Typical Infrastructure Description

A typical supported site may include COTS/GOTS hardware and software; COTS/GOTS communication and supporting security equipment; intelligence data handling and C4IM Systems including: Local, Metropolitan, and Wide Area Networks; secure and non-secure video teleconferencing systems; communication devices, storage devices, workstations and servers (of different types, such as email and Web servers); printers, copiers, scanners, and facsimiles; telephones, smart phones, wireless devices, Voice Over Internet Protocol (VoIP) phones, badge readers, digital senders, and related support devices necessary for the sites' effective operation.

1.1.4 Glossary

1.1.4.1 Contracting Officer (KO)

The Procuring Contracting Officer is the person with the authority to enter into, administer, and/or terminate contracts and make related determinations and findings. The term includes certain authorized representatives of the contracting officer acting within the limits of their authority as delegated by the contracting officer. "Administrative contracting officer (ACO)'' refers to a contracting officer who is administering contracts. The Contracting Officer is the only individual who can legally bind the government.

1.1.4.2 Preventative Maintenance

Preventative maintenance is the care and servicing by contractor personnel for the purpose of maintaining equipment in operating condition in accordance with manufacturer's commercial specification by providing for systematic inspection, detection, and correction of incipient failures either before they occur or before they develop into major defects.

1.1.4.3 Remedial Maintenance

Remedial maintenance is the act of restoring an item to a state in which it can perform its required function. It includes all technical and corresponding administrative, managerial, and supervisory actions to achieve service restoration.

1.1.4.4 System Maintenance and Repair

All efforts required to ensure availability of C4IM Systems consistent with the manufacturer's performance specifications and the intended use of the system in support of the mission.

1.1.4.5 Systems Operations

System Operations is defined as all efforts required to provide the day-to-day routine monitoring, operations planning, and operation of the C4IM Systems to ensure customers enjoy reliable, uninterrupted access and availability.

1.1.4.6 Communications

Is defined as all tactical and non-tactical communications to include telephone, satellite, infrared, various radio, various frequency (UHF, VHF, etc.), cryptochannel, telephones, wireless and military spectrum management.

1.1.4.7 Configuration Management

Configuration Management (CM) is defined as the process during which the changes of a C4IM System are implemented in a controlled manner by following a pre-defined framework/model.

1.1.4.8 Information Assurance

Information Assurance (IA) is the protection of systems and data in storage, during processing, or in transit from unauthorized access or modification; denial of service to unauthorized users; and the provision of services to authorized users.

1.1.4.9 Information Assurance Vulnerability Alerts (IAVA)

IAVA are tasks and directives received by the units from the Joint Task Force-Global Network Operations, Defense Intelligence Agency (DIA), or Defense Information Systems Agency (DISA), and direct DoD and IC organizations to correct IT vulnerabilities.

1.1.4.10 System Availability

System Availability is defined as the degree to which an IT system is operable and in a committable state. It is the proportion of time a system is in a proper and full useable functioning condition.

1.1.4.11 Threshold for Performance Restoration Period (TPRP)

The TPRP is the period of time during which the contractor shall restore the operational capability. The period begins from the point at which the contractor is notified of system failure and ends upon full restoration of its original equipment manufacturer (OEM) capability for use.

1.1.4.12 Critical Systems

Critical Systems is defined as the following:

- Email servers,
- Web servers (and supporting data servers),
- Storage Area Networks (SANs)
- Network and Communications Infrastructure (to include at a minimum, infrastructure fiber and/or copper network cables, routers, switches, and cryptographic equipment), and
- Other systems identified by the Government.

1.1.4.13 Mission Essential Personnel

Mission Essential Personnel, for the purposes of tasks included in this PWS, are those responsible for ensuring the C4IM capabilities the Government considers basic and necessary for the accomplishment of the organization's mission remain operational during installation or Government closure. Mission Essential Personnel will be identified by site.

1.1.4.14 Transition Activities

Transition Activities are defined as the efforts required to begin the execution of assignments under this task order and to close out those efforts when the task performance ends in a timely and efficient manner.

1.2 Scope

The contractor shall provide the full range of C4IM sustainment and technical support services to ensure uninterrupted service to INSCOM, Army G2, ARCYBER, and mission partners within the Continental United States (CONUS) and Outside the Continental United States (OCONUS). The systems supported under this Performance Work Statement (PWS) consist of commercial, modified-commercial and specially designed equipment items.

1.3 Period of Performance

The government anticipates award of multiple IDIQ contracts with a five (5)-year ordering period. Task orders will have one (1)-year base period and may have up to four (4) option periods (no option period will exceed one (1)-year in duration), however, the period of performance will not extend beyond 364 days after the last ordering day of the IDIQ contract to include option to extend services.

1.4 Place of Performance and Hours of Operation

The KO is located at the following address: 8825 Beulah Street, Fort Belvoir, VA. Other locations may be worldwide, but generally are represented in the G6 Enterprise Functional Breakdown by Unit matrix.

1.4.1 Central Site/Remote Locations. Each unit has a central site and many have remote sites. The contractor shall be responsible for providing support to all of these locations.

1.4.2 Core performance hours for the places of performance within this contract will be identified at the task order level.

1.5 Type of Contract

TBD

2.0 PERFORMANCE OBJECTIVES

The contractor shall provide all support necessary to ensure all IT Systems accountable under the task order meet Original Equipment Manufacturer (OEM) established standards, Government-specific technical requirements, and established operational functions necessary to support the user. The contractor shall provide eleven principal services: 1) network operations, 2) operational maintenance, 3) storage management, 4) service desk, 5) information assurance, 6) engineering & installation, 7) database services, 8) communications, 9) system engineering and technical assistance support and 10) visual information and multimedia engineering support. The C4IM Service Catalog is considered a baseline of service requirements, but may be adapted by sites.

The CIO/G6 ENTERPRISE Performance Requirements Summary (PRS) identifies the quality of service requirements for this PWS; see attachment xx-xx.

2.1 Network Operations

The contractor shall plan for implementing all Government approved Original Equipment Manufacturer (OEM) and Government mandated releases and updates as necessary to meet system performance requirements and interfaces with external systems and networks. This planning requirement is twofold. First, the contractor shall anticipate update requirements by staying abreast with industry developments and trends and Government initiatives that are relevant to the components of the C4IM Systems. Secondly, the contractor shall plan for and schedule updates and maintenance to minimize service disruptions and accommodate the unit specific Government approvals and configuration management processes. The contractor shall operate the C4IM Systems to ensure reliable, uninterrupted access and availability as required in order to execute their mission. System operation during surge requirements (i.e., in support of exercises or other mission essential activities) shall be as directed by the Government. The contractor shall provide preventative and remedial maintenance for the site's C4IM Systems. The contractor shall provide and ensure the availability of the C4IM Systems consistent with OEM's performance specifications and the intended use of the system in support of the site's

mission. The C4IM Service Catalog is considered a baseline of service requirements, but may be adapted by sites.

2.1.1 System, Network, Web and Database Administration. The contractor shall perform administration, maintenance, diagnosis and restoration on all C4IM systems, databases, web applications and networks.

2.1.2 System Backup. The contractor shall conduct scheduled backups of the site's data (on all networks) in accordance with the unit's operational and business requirements. This effort includes the management and operations of the site's Storage Area Network and/or Network-Attached Storage (as appropriate) and replication of off-site data IAW unit SOPs.

2.1.3 Network Monitoring. The contractor shall perform all of the requirements to actively monitor the performance of the C4IM System at the central site and remote location(s) to ensure it is operating efficiently and customers have the capabilities needed for mission execution. The contractor shall identify trends of degrading performance and facilitate fault isolation and preventative and remedial maintenance as appropriate. The contractor shall notify the site's leadership identified by the ACOR when the System experiences a component failure. The contractor shall receive and prepare electronic notifications to the command on all scheduled network outages. The contractor shall monitor services on all local and wide area networks for optimum operability using a variety of network monitoring tools, report outages, and initiate support within 30 minutes of initial loss of service. The contractor shall gather information and track outages until connectivity is restored and provide updates until systems are fully restored,

2.1.4 Record Messaging. The contractor shall provide administration and maintenance of the Multimedia Message Manager (M3) or other designated secure messaging capability.

2.1.5 Account Management. The contractor shall provide account administration and maintenance for all applicable accounts.

2.1.6 Server/System Administration. The contractor shall provide server virtualization administration and maintenance for the virtual environments (i.e., virtual private servers, guests, instances, containers or emulations).

2.1.7 LAN Administration. The contractor shall provide LAN administration using government provided products and provide daily system and mail administration as delegated by Government administrators such as creation, maintenance and deletion of user email accounts in accordance with the local SOPs. Interface to centrally managed mail systems such as mail.mil will be required.

2.1.8 Enterprise Active Directory Management. The contractor shall provide Active Directory (AD) network and security administration and maintenance for all domain controllers. Contractor shall be responsible for authenticating all users and computers within a network of Windows domain type, assigning and enforcing security policies for all computers in a network and installing or updating software on network computers.

2.2 <u>Operational Maintenance</u>. The contractor shall perform scheduled maintenance to ensure consistent and reliable service availability to customers. The requirement to perform specific scheduled maintenance may result from manufacturers recommended service intervals, alerts and bulletins, available patches and updates, directions from the unit's change management process, as well as other sources (to include Information Assurance Vulnerability Alerts). The C4IM Service Catalog is considered a baseline of service requirements, but may be adapted by sites.

2.2.1 Change Management. The contractor shall ensure all IT system changes are captured IAW local change management processes and systems and will provide visibility to any devices being attached to the network. The contractor shall follow change management regulations for all purchases and services and coordinate at the unit level through the unit change management authority. Changes may include, but are not limited to changes to the unit's mission objectives; directives from Army, DoD, or the IC; OEM best business practices or warranty requirements; release of new technology; advances in commercial/Government technology or contractor recommendations. Contractor shall ensure that all software and hardware is net worthy, maintained and documented.

2.2.2 Hardware Management

2.2.2.1 Asset Management. The contractor shall maintain the site's hardware asset inventory in the Government's Army System Integration Database (ASID) or other database as directed. The contractor shall employ ASID in accordance with the site's IT service-level management processes and inventory controls. The contractor shall support the unit's equipment receipt and control management business process. The contractor shall document, manage, and maintain the sites hardware baseline and manage and maintain a configuration library for the site's configuration documentation identified by the unit change management authority.

2.2.2.2 Cable Plant Management. The contractor shall update and maintain an active database of cable plant configuration and label cables appropriately to ensure accurate identification of cable locations and equipment supported by that cable. The contractor shall install, maintain, manufacture and reconfigure as necessary.

2.2.2.3 Capital Equipment Replacement Program (CERP). The contractor shall support the unit's equipment replacement program. This can include, but is not limited to: ASID management; listing all unit C4IM equipment; developing a plan on CERP criteria (age, serviceability, reparability, cost savings, criticality, etc.) and making recommendations to the unit's emerging technical and architectural requirements.

2.2.2.4 Equipment Installation. The contractor shall perform installation/de-installation of supporting hardware including, but not limited to personal computers, communications closet components and all associated infrastructure supporting the networks in response to automation work requests. No refurbished equipment shall be utilized without prior government authorization. The contractor shall install and de-install hardware and software as required to ensure consistent and reliable service availability to customers. Installations and de-installations may result from repairs, replacements, or other maintenance actions. All installations and de-installations shall be in accordance with manufacturer and/or unit specific instructions. De-

installed components and software will be sanitized per appropriate security procedures. All installations shall include appropriate functional verifications to ensure serviceability and documentation IAW change management authorities.

2.2.2.5 Update/repair/replace (break fix) system hardware. The contractor shall repair and/or replace system hardware as required to ensure consistent and reliable availability to the site customers (as defined by OEMs and industry best practices, and Federal/DoD mandates). Repair/replace actions may result from a notification (e.g. trouble ticket) and/or malfunction discovered by the system operations staff. The contractor shall track each repair or replacement action from identification through completion of repair or replacement and functional/system verification to ensure all repairs or replacements are completed accurately and in a timely manner utilizing local unit's change management system

2.2.3 Software Management. The contractor shall provide software management support, in accordance with the change management process, which requires knowledge of current and emerging technologies and trends in the software field, knowledge of inventory, licensing and configuration management procedures as applied to software architecture.

2.2.3.1 Software Licensing Revalidation. The contractor shall support the software standards and compliancy program. This includes implementing control procedures for updating software baseline documentation as required. Perform research to ensure the latest approved software versions are being used. The contractor shall assist the local unit's software manager to ensure that no lapses in software licenses occur that may affect mission operations.

2.2.3.2 Software Enterprise License Management

2.2.3.2.1 The contractor shall conduct periodic software baseline verification inventories to correct documentation deficiencies and perform on-the-spot audits of unit computer systems documenting findings as required in support of DoD software compliancy directives. The contractor shall keep an accurate, updated inventory of all software licenses to include volume licenses, site and enterprise agreements and shall ensure that media and/or software distribution processes are in place for software installation world-wide. This process could include packaging and mailing media where required or utilizing vendor- supported distribution web-sites.

2.2.3.2.2 Utilizing ITIL best practices, the contractor shall support management of the software media library which includes receiving new software, updating the software tracking database, creating back-up copies of software, and filing software in the library. The contractor shall determine and dispose of obsolete software in compliance with applicable disposal policies while ensuring that software requirements are properly staffed through existing requirements approval processes. The contractor shall coordinate with Army Small Computer program to determine if software is available through the Enterprise Software Initiative (ESI) and secure required waivers, as appropriate, and serve as the alternate Licensing Benefits Administrator for the Microsoft Licensing Web-site, setting up or deleting accounts and providing or removing privileges in accordance with guidance from the Software Manager or established procedures.

2.2.4 On-Call Support. The contractor shall provide "on-call support" during other than normal duty hours, publish a monthly on-call roster for all personnel on the team, contact the IT government lead within local designated time for on call support services and report in person to the designated/affected site to resolve issues or problems that are not resolved by telephone. The contractor shall physically report to the designated/affected site.

2.2.5 Business Processes

2.2.5.1 Information Technology Infrastructure Library (ITIL) Implementation. Contractor shall support and assist in implementing ITIL best practices into C4IM processes to improve efficiency.

2.2.5.2 Business Case Analysis. The contractor shall use business case analysis tools to develop plans to improve processes, efficiency and effectiveness.

2.2.5.3 The contractor shall assist the Government representative in conducting organization inspections.

2.3 <u>Storage Management</u>. The contractor shall support tools, processes, and policies used to manage and administer global and local enterprise storage systems to sustain and enhance the capabilities of the infrastructure.

2.3.1 Emergency Data/Disaster Recovery. The contractor shall provide emergency data recovery services which includes, but is not limited to, hard drive/solid state drive recovery, raid data, exchange server, SQL database repair, and tape data retrieval. The contractor will ensure continuation of operations (COOP) in accordance with local COOP plans.

2.4 <u>Service Desk</u>

2.4.1. The contractor shall provide service desk and technical support to address unit system and communications problems. It will be integrated with a unit monitoring/tracking system.

2.4.2 The contractor shall provide surge labor support during contingency/emergency or other mission support operations.

2.4.3 The contractor shall operate the Common Access Card (CAC) reset.

2.4.4 The contractor shall use trouble tickets to log calls and is responsible for timely processing of all trouble tickets opened within the established standards. The contractor shall ensure all necessary data within the trouble tickets is appropriate for proper troubleshooting and monitoring. The contractor shall provide customers a ticket number when a request for assistance is received.

2.4.5 The contractor shall immediately report any problems the local service desk has investigated and cannot resolve to the appropriate support office for final resolution in accordance with established SOPs. The contractor shall determine complexity of the problem

and whether or not the ticket should be immediately referred higher or if expertise exists locally to resolve the issue expeditiously and accurately.

2.5 Information Assurance (IA). The contractor shall provide IA support to include, but is not limited to, measures necessary to detect, document, remediate and counter IA threats as directed by the unit's Information Assurance Manager (IAM). The contractor shall provide advice and guidance and service support concerning Information Assurance (IA) matters as required. The contractor shall enforce all aspects of the Army Information Assurance Program to include COTS, GOTS, freeware, shareware, Program Management (PM)/Major Command (MACOM) fielding's, local unique, beta tests, application and system development, network access, IT acquisition policies, connectivity, IA tools utilization, and authorized software and system management controls.

2.5.1 Accreditations. The contractor shall provide services in support of all Information Security guidance, processes and policies. Contractor shall provide support to the Information Assurance Manager (IAM) in ensuring all C4IM systems are properly certified and accredited.

2.5.1.1 The contractor shall perform IA IT assessments of all current and future C4IM systems and develop risk management guidelines.

2.5.1.2 Authorization to Operate. The contractor shall support maintenance of the unit's Authorization to Operate (ATO) for all networks. The contractor shall maintain the security posture of the unit's IT System in accordance with the certification and accreditation (C&A) package, the supporting Plan of Action and Milestones (POA&M), and the appropriate accrediting authority.

2.5.2 Compliance Management

2.5.2.1 The contractor shall ensure IT devices and networks are Army Information Assurance Vulnerability Management (IAVM) and Anti-Virus Program (AV) compliant. This includes, but is not limited to, IAVM acknowledgment, patching, updates, completion and reporting of all other corrective actions within specified timelines as required by the accrediting authority.

2.5.2.2 The contractor shall ensure that log files and audits are maintained and reviewed for all systems and that authentication policies are audited for compliance.

2.5.2.3 Federal Information Security Management Act (FISMA). The contractor shall ensure the unit's compliance with the requirements set forth in the FISMA. These requirements include maintaining and/or achieving a valid ATO for each of the unit's networks; completion of the annual unit's Self-Assessment Security Readiness Review; completion of annual testing of security controls; and annual evaluation of contingency plans. The contractor shall submit FISMA reporting data and documentation on all of the unit's networks as directed.

2.5.2.4 HBSS. The contractor shall provide assistance with development, implementation and operations of Host Based Security System (HBSS) at various sites throughout the enterprise.

2.5.3 Firewalls. The contractor shall provide installation and maintenance of the firewall solutions, assignment/maintenance of user accounts, interfacing with the network proponent for network changes/modifications and assessing impacts on the user community, and analysis of connectivity problems and resolution.

2.5.4 Security Operations

2.5.4.1 The contractor shall report information systems security violations and incidents to the appropriate authority. The contractor shall review and evaluate the effects of security on system changes, document results and assist the IAM in remediation and restorative processes.

2.5. The contractor shall collect, document, and turn in for destruction all applicable media and hardware.

2.5.5 IA Security Officer. The contractor shall serve as and perform the duties of the unit's IA Security Officer as directed by the Government and unit Information Assurance Manager (IAM).

2.6 <u>Engineering and Installation</u>.

2.6.1 Site Surveys. The contractor shall perform on-site or desktop engineering surveys to obtain engineering, environmental, and physical plant data required for use in the preparation of Engineering Installation Package (EIP) technical documentation and Information Systems Cost Estimate (ISCE) in Military Construction, Army (MCA) and Unspecified Minor Military Construction Army (UMMCA) projects and local site projects. The contractor shall prepare IT, voice, facsimile, video, Internet Protocol (IP), and data communications equipment installation documentation to include floor layouts, lists of major items of equipment and bills of material (BOM), rack face elevation drawings, schematic drawings reflecting equipment interconnection and terminations, cable cut-sheets, labeling, duct layouts, engineering and installation specifications and as-built documentation as required by orders in accordance with 9th Army Signal Command (NETCOM) and unit configuration management regulations. The duct layouts and schematic drawings shall uniquely identify all cable plant component locations and logical schematics. The layouts shall uniquely identify all components, including a facilities description that clearly defines all operations, procedures, facilities, and capabilities. The contractor shall provide documentation diagrams including inventories for each client's entire network configuration, where appropriate. Documentation shall be performed IAW DoD, DA and IC standards.

2.6.2 Engineering Implementation Plan (EIP)

2.6.2.1 The contractor shall work directly with engineers, area installation, and operational personnel to ensure that all systems installation and reconfiguration issues are managed quickly and accurately.

2.6.2.2 The contractor shall provide an EIP which includes maintaining a current listing of technical installation specification and documentation of C4IM systems.

2.6.2.3 The contractor shall initiate, at government request, the process and continued coordination to obtain Long-Haul Information Transfer Services, in accordance with DoD, DA, and IC standards, supporting major command exercises, deployments and new equipment fielding in support of worldwide user requirements.

2.6.2.4 The contractor shall review and recommend new and existing circuits for alternative routing to balance loading between the systems and/or cost and efficiency improvements.

2.6.3 Installation and Testing. The contractor shall conduct acceptance testing and transition in accordance with the Government approved test and acceptance plans contained in the EIP.

2.7 Workflow, Web and Database Services. The contractor shall design, develop, test, operate, enhance and maintain applications in accordance with established policies, regulations, and guidelines. The contractor shall conduct training sessions for individuals and groups of users as required. Update and maintain all user manuals, quick reference guides, on-line help, and multi-media tutorials for all modules in the data systems. The contractor shall design, develop, test, operate, enhance and maintain the database management systems (DBMS).

2.8 Communications. The contractor shall provide support to all tactical and non-tactical communications.

2.8.1. Tech Control. The contractor shall install, deinstall, test, monitor, maintain, troubleshoot and repair from unit to enterprise level network connectivity, telecommunications systems & equipment, communication systems & equipment, communications security equipment and associated terminal and ancillary equipment and supporting cable, duct and conduit systems. Contractor shall conduct acceptance testing and cutover in accordance with government approved acceptance plans and handoff.

2.8.2 COMSEC Support. The contractor shall be responsible for monitoring, operation, and coordinate for repair of COMSEC equipment. The contractor shall perform COMSEC support activities and functions defined by the COMSEC Custodian and the unit's business processes. The COMSEC Custodian will be familiar with Encryptor hardware and appropriate regulations.

2.8.2.1 The contractor may serve as the temporary Alternate COMSEC Custodian as directed.

2.8.2.2 The contractor is responsible for the establishment and operation of the crypto network, including validating crypto net key requirements and user profiles.

2.8.2.3 The contractor shall provide support to the Government COMSEC custodian for the supervision and oversight of all sub-accounts and hand-receipt holders (HRH) to ensure compliance with existing COMSEC material security, accounting, and operational policies/procedures.

2.8.2.4 The contractor shall provide support for the management and administration of the accounting, maintenance, handling, storage, distribution , receipt, COMSEC message

coordination and destruction of COMSEC equipment and material in accordance with appropriate guidelines.

2.8.2.5 The contractor shall provide guidance and advice for COMSEC integration and configuration management supporting requirements, programs, and projects.

2.9 Systems Engineering and Technical Assistance (SETA) Support. The contractor shall leverage high quality, state-of-the-art, advanced science, analytical, systems engineering and technical services, and Army knowledge expertise to meet the unit's mission to support the Army, DoD, Intelligence Community and the Warfighter. Within the SETA construct, the contractor will be engaged in an environment focused on supporting Army and Intelligence Community transformation, the Overseas Contingency Operations, and current operations. The contractor must have knowledge and experience in strategic, operational, and tactical military intelligence and supporting C4IM requirements including intelligence systems and supporting communications systems.

2.9.1 The contractor shall have knowledge and development experience in the following applications:

a. Microsoft Office Suite
b. Microsoft SharePoint
c. Microsoft Project
d. Microsoft Visio
e. C++
f. Current Windows Operating Systems
g. Microsoft Active Directory Services
h. Microsoft SQL

2.9.1.1 The contractor shall participate verbally and in writing in the staffing of memorandums, letters, executive summaries, information papers, discussion papers, read-ahead packets, and trip reports; presenting information and decision briefs at all audience levels from user to the Commanding General.

2.9.1.2 The contractor shall draft policy documents needed to implement C4IM related policy developed by the DOD, NSA, DIA, DoDIIS and HQDA. The Government shall review and approve final policy documents.

2.9.2 The contractor shall use the Army Records Information Management System (ARIMS) at all times when filing documents. (ARIMS replaced the Modern Army Record Keeping System (MARKS)).

2.9.3 The contractor shall support the creation and maintenance of comprehensive enterprise solutions for collaboration, information discovery, information access and information sharing. This will include the procurement, development, management and maintenance of a collaborative KM Portal solutions. This work will be completed with efficient management and

maximization of existing and future C4IM investments. The contractor shall support knowledge management activities by enabling related C4IM plans and solutions.

2.9.4 The contractor shall support the development of business cases and associated framework standards needed to comply with AR 25-1 and the Clinger-Cohen Act of 1996, also known as the Information Technology Management Reform Act (ITMRA).

2.9.5 The contractor shall support the review of C4IM initiatives and ongoing projects and present recommendations to delay, modify or terminate those based upon risk-value analysis of the overall IT portfolio and support initiatives as a catalyst for change, growth and improvement. This support will include input on C4IM performance planning, training/facilitation, recommending solutions to inefficient business processes, developing supporting case studies which apply appropriate metrics, and implementing approved solutions. These initiatives include the consolidation, aggregation, interfacing, integration and interoperability of data and information across the C4IM architecture. The contractor shall maintain cognizance of, and leverage as appropriate, industry and Government C4IM advances.

2.9.6 The contractor shall assist with implementation of Information Technology Infrastructure Library (ITIL) compliant IT Service Management (ITSM) processes, and provide support to assigned process owners and managers implementing standard ITIL v3 processes: Service Strategy, Design, Transition, Operation and Continual Improvement. The position will be responsible for planning and tracking ITIL implementation, and assessing IT operational maturity, strategy, design and implementation across the services management processes. The contractor will interface with process owners and senior IT leaders to facilitate business rules and coordinate integration of related functions.

2.9.7 The contractor shall support enterprise IT Capital Planning and Investment Management, IT Portfolio Management, and the IT Capital Equipment Replacement Program. The contractor shall support the lifecycle change management and replacement process for hardware and software. The contractor will evaluate compliance with governance policies in preparation of future expenditures. The contractor will support a strategy or plan to allocate C4IM resources to support mission priorities.

2.9.8 The contractor shall support functional requirement development and technical solution implementation supporting Business Process Reengineering and Lean Six Sigma initiatives.

2.9.9 The contractor shall fully understand and be able to provide SETA support for related functions listed in the following documents:

a. Army Knowledge Management (AKM) Guidance
b. Army Information Management AR 25-1
c. INSCOM CIO/G6/S6 IT/IM Strategic Plan
d. INSCOM CIO/G6/S6 Implementation Plan
e. INSCOM Regulation 10-2 INSCOM Regulation 25-70 (Supplements AR 25-1) Acquisition and Management of Information Resources
f. NSA Enterprise Solutions (NES) Strategy and Implementation Plan

g. DoDIIS Strategic Plan
h. Army Regulation 25-2, Information Assurance
i. Federal Information Security Management Act (FISMA)
j. Clinger-Cohen Act of 1996 (Information Technology Management Reform Act or ITMRA)
k. EO 13011(Federal Information Technology)
l. OMB Circular A-11, Part 3, Planning, Budgeting and Acquisition of Capital Assets, Office of Management and Budget
m. DoD 5000 Series (DoD Directive 5000.1 and Instruction 5000.2)
Global Network Enterprise Construct (GNEC)
n. Site specific/local policies and SOP's

2.9.9.1 The contractor shall be well versed in the rules and regulations governing the storage (all mediums) and protection of classified information.

2.10 <u>Visual Information/ Multimedia Resource Planning Support.</u> The contractor shall provide coordination support for VI/Admin Division customer planning meetings conferences, expositions and trade shows. The contractor shall develop meeting requirements and support recommendations, provide site event support and coordination with cross-functional teams as appropriate, and complete after actions reports.

2.10.1 VTC Operational and Technical Support. The contractor shall provide all necessary technical support for the following:

- Room Based VTC Support
- Operator-Level Equipment Sustainment Support
- Desktop VTC Support
- Desktop VTC Compliance Services
- Desktop VTC Expertise Support
- Desktop VTC Capability Operational Support

2.10.2 Multimedia Production, Presentation and VTC Support. The contractor shall provide support to multimedia environments and facilities. This shall include, but is not limited to:

- Presentation and Conference Room Support Services
- Pre-Meeting Support
- Facility Planning and Preparation Support

2.10.3 Multimedia Production Support. The contractor shall provide the support for video, photographic and graphics production. This shall include, but is not limited to:

- Video-Specific Production Support
- Graphics and Production-Specific Support
- Production Technical Support

- Technology Modernization Support
- Multimedia Production Administrative Support
- Photographic-Specific Support
- Extraordinary Operations Planning Support
- Multimedia Standalone Local Area Network Support

2.10.4 Engineering & Design of VTC and Multimedia Systems Support. The contractor shall provide short and long-term engineering and planning of technology enhancements, extensions, innovations and refreshment services to include:

- Engineering Planning and Design.
- Engineering Execution.
- Engineering Configuration
- Engineering Training
- Engineering Equipment Documentation
- Multimedia Help Desk and Maintenance Support

2.10.5 Closed Circuit and Commercial Media Services. The contractor shall provide:

- Commercial Media Services
- Media Distribution Capability Sustainment
- Audio and Video Signal Configuration Services
- VI/Multimedia Resource Planning Support

2.10.6 VI/Multimedia Resource Planning Support. The contractor shall provide:

- Meeting Support Planning
- Meeting Requirements and Support Recommendations Development
- Site Event Support and Coordination
- Staff Inspection Program Support
- Coordination of Annual Training Requirements

2.11 Key Personnel. Key Personnel are identified as the Contractor Program Manager and all Site Leads. The contractor shall notify the KO prior to making any change in key personnel.

2.12 Transition Activities. The contractor shall provide transition activities for the phase-in period beginning at task order award. The phase-out period begins upon KO notification. (Note: All exchanges of information between the incoming and outgoing contractors, and between the Government and the contractors shall be conducted through the KO, COR, or ACOR as appropriate.)

2.12.1 Transition Planning. The contractor shall develop a phase-in which addresses both phase-in and phase-out for the INSCOM CIO/G6 ENTERPRISE task order at each unit. The transition

plan shall address all activities associated with contractor provided services and be delivered to the KO, COR, and unit's ACOR. The transition plan shall be updated 60 days prior to the expiration of a performance period unless otherwise noted or directed by the KO. The KO will coordinate with the U.S. Forces in the respective host nations to determine the appropriate contractor status under the SOFA in compliance with the applicable regulations and agreement between the U.S. and the host nations. (for Japan, if applicable).

2.12.2 Phase-In Activities. The contractor shall perform the following activities per the task order during the phase-in period as slated in the contractor's approved phase-in:

- Submit requests for physical and network access at performance locations
- Submit requests for security clearance documentation and other items requiring responses from the Government
- Perform joint inventories and inspections of all Government Furnished Equipment (GFE), facilities and property with the Government and outgoing contractor
- Validate the authoritative list of IT equipment (hardware and software) with the Government and outgoing contractor
- Coordinate with the Government to validate or establish requirements and associated performance objectives for services
- Establish procedures with the predecessor to ensure transition of provided services without any degradation of service
- Receive from predecessor copies of all instructions, records, databases, task order performance metric data, vendor points of contact, and all other procedures developed by the predecessor in the performance of the task order(s)
- Perform identification and inventory of all contractor maintained classified data relevant to the performance of the task order

2.12.3 Phase-Out Activities. The contractor shall perform the following activities for the task order during the phase-out period per the contractor's transition plan:

- Ensure all services and performance objectives required by the PWS and task order are met throughout the phase-out period
- Establish procedures with the successor to ensure transition of provided services without a degradation of service
- Provide copies of all instructions. records, databases, task order performance metric data, vendor points of contact, and all other procedures developed by the contractor in the performance of this task order to the successor
- Update and validate the authoritative IT equipment (hardware and software) list with the Government and the successor
- Perform joint inventories and inspections of all GFE, facilities, and property with the Government and the successor
- Turn over to the each unit’s ACOR all GFE and supplies

2.13 Quality Assurance

2.13.1 Contractor Quality Responsibility. The contractor shall be responsible for the quality of all work performed by contractor personnel and shall guarantee all workmanship provided by the contractor regarding repair of all hardware and software for a period of 30 days, except for the fault or negligence of the Government, or causes external to the equipment. Within this 30-day period, the contractor shall furnish travel, per diem, labor and material at no additional charge to correct material or workmanship faults.

2.13.2 Quality Control Plan (QCP). The contractor shall prepare a QCP which includes provisions for bi-annual surveys to determine customer satisfaction with all contractor provided services, and in accordance with the Government's QASP, Attachment A. The contractor shall submit a survey plan, detailing the survey questions, how the survey will be conducted, to whom the survey will be furnished, and how the results will be collected, analyzed and reported, as part of its response to this solicitation. Data and analysis of the survey results together with the Contractor's plans and recommendations to improve service for deficient areas will be submitted for approval to the COR/ACOR and the unit leadership within 30 days of survey completion.

2.14 Responsibilities. The Government representatives responsible for quality assurance of performance are:

2.14.1 Contracting Officer (KO). The Contracting Officer ensures performance of all necessary actions for effective contracting and ensures compliance with the terms of the contract and safeguards the interests of the United States in the contractual relationship. It is the Contracting Officer that assures the Contractor receives impartial, fair, and equitable treatment under the contract. The Contracting Officer is ultimately responsible for the final determination of the adequacy of the Contractor's performance.

2.14.2 Contracting Officer Representative (COR)/Alternate Contracting Officer Representative (ACOR). The Contracting Officer Representative/ Alternate Contracting Officer Representative is responsible for administration of the project and assures proper Government surveillance of the Contractor's performance. The COR/ACOR is not empowered to make any contractual commitments or authorize any contractual changes on the Government's behalf. Any changes that the Contractor deems may affect contract, price, terms, or conditions shall be referred to the KO for action.

2.15 Escort Requirements. Contractors may be required to escort non-cleared personnel into SCIF or SAP locations for the purpose of identifying and rectifying problems with software or hardware operated and maintained under this PWS or for facility maintenance as required and validated by the site ACOR.

2.16 Security Requirements

2.16.1 Contractor personnel must have and maintain a TOP SECRET/SCI clearance. Personnel must sign a Non-Disclosure Statement. Personnel must perform within the security limitations of AR 381-10, USSID 1800, and other appropriate security regulations according to their intelligence disciplines.

2.16.2 All individuals requiring access to information technology (IT) systems will have the appropriate security clearance and will be granted access according to their security clearance, need-to-know and their IT position/category. Additional position category and investigation guidance is available in DOD 5200.2-R. As referenced from AR 25-2, personnel requiring access to information systems processing classified information to fulfill their duties will possess the required favorable security investigation, security clearance, formal access approval (DoD Directive 8570) and need to know. ADP/IT tier level positions are detailed in the task orders. (DoD Directive 8570) ADP/IT positions are as follows:

ADP-III / IT-III

2.16.3 **Additional Security Requirements.** This effort requires access to classified Government information at U.S. Government only. Additional requirements are contained in the DD Form 254. Additional security requirements may be added at the task order level. All personnel working on-site in any of the Government facilities will maintain a Top Secret/SCI (TS/SCI) or Secret security clearance as required.

2.16.4 **Special Requirements**

2.16.4.1 Contractor Personnel Required Experience, Training and Certification. The contractor shall ensure all personnel assigned possess appropriate experience, training and certification. The minimum requirements include:

a) Contractor personnel supporting this effort must possess sufficient technical certifications, educational degrees, and experiences levels consistent with the requirements of the task that an individual employee will perform.

b) Contractor personnel supporting this effort must have minimum certifications in accordance with DoDD 8570, Army Regulation 25-2 and the 7th SC (T) CE Certification Matrix.

c) Minimum level of experience required to perform specific tasks at this site; the personnel structure for the TNCC at minimum will be broken down into 3 levels:

- Level 3: Shift Lead:

  - Minimum experience level of 7 yrs

  - Contractor certification(s) required for advanced user privileges will be based on IAT Level II and IAM Level I IAW DoD 8570.01-M.

- Level 2: Senior Technician:

  - Minimum experience level of 5 yrs

  - Contractor certification(s) required for advanced user privileges will be based on IAT Level II IAW DoD 8570.01-M.

- Level 1: Technician

  - Minimum experience level of 5 yrs

  - Contractor certification(s) required for advanced user privileges will be based on IAT Level I IAW DoD 8570.01-M.

2.17 Constraints

Compliance with appropriate Army and DOD regulations, DISA, National Institute of Standards and Technology (NIST), Federal Information Security Management Act (FISMA), Government Performance and Results Act of 1993 (GPRA), and Clinger-Cohen (formerly Information Technology Management Reform Act - ITMRA) is required. Compliance with the following documents also apply to this contract:

TABLE 1 - CONSTRAINTS

NO.	ID	NOUN NAME/URL REFERENCE
1	ACERT Tools	ACERT TOOLS; https://www.acert.1stiocmd.army.mil/tools/
2	AR 25-1	Army Knowledge Management and Information Technology; http://www.apd.army.mil/pdffiles/r25_1.pdf
3	AR 25-2	Information Assurance; http://www.apd.army.mil/pdffiles/r25_2.pdf
	AR 380-40	Safeguarding and Controlling Communications Security Material**.**
4	AR 380-53	Information Systems Security Monitoring; http://www.apd.army.mil/pdffiles/r380_53.pdf
5	AR 525-13	Antiterrorism 4 Jan 2002; http://www.apd.army.mil/pdffiles/r525_13.pdf
6	AR 530-1	Operations Security 19 Apr 2007; http://www.apd.army.mil/pdffiles/r530_1.pdf
7		BBP Index; https://informationassurance.us.army.mil/bbp/
8		BBP Index Drafts; https://www.us.army.mil/suite/kc/585383
9		BBP Army Password Standards Version 1.5; https://informationassurance.us.army.mil/bbp/army_password_standards.pdf
10		BBP Web Filtering; https://informationassurance.us.army.mil/bbp/web_filtering.pdf
11		BBP Wireless Security Standards Version 2.0; https://informationassurance.us.army.mil/bbp/bbp_wireless_final.pdf
12		BBP Reuse of Army Computer Hard Drives v1.1; https://informationassurance.us.army.mil/bbp/computer_hard_drives.pdf

13	CJCSM 6510	http://www.dtic.mil/cjcs_directives/cjcs/manuals.htm
14		CNDSP C&A Evaluator Standard Operating Procedure; https://powhatan.iiie.disa.mil/cnd/CNDSP_SOP_V1.3A_20040304.pdf
15		CNDSP Evaluator's Scoring Metrics CERTIFICATION AND ACCREDITATION of Computer Network Defense Service Providers; https://powhatan.iiie.disa.mil/cnd/esm-v60-dtd100206.doc
16	DA PAM 25-5	Preparing and Processing Request for Long-Haul Information Transfer Services.
17	DA Pam 25-6	Configuration Management for Automated Information Systems; http://www.doim.army.mil/Regulations_Pams_Directives/p25_6.pdf
18	DCID 6/3	Director of Central Intelligence Directive 6/3 Protecting Sensitive Compartmented Information Within Information Systems http://www.fas.org/irp/offdocs/DCID_6-3_20Manual.htm
19	DJSIG	DoD Joint Security Implementation Guide (DJSIG).
20	DOD 5220.22-M	Department of Defense (DOD) 5220.22-M, National Industrial Security Program Manual (NISPOM)
21	DODD 5200.1	DoD Information Security Program; http://www.dtic.mil/whs/directives/corres/pdf/520001p.pdf
22		DOD Policy Web Site Administration and Procedures; http://www.defenselink.mil/webmasters/policy/dod_web_policy_12071998_with_amendments_and_corrections.html
23	DODD 8500.1	Information Assurance (IA); http://www.dtic.mil/whs/directives/corres/pdf/850001p.pdf
24	DODD 8500.2	Information Assurance (IA) Implementation; http://www.dtic.mil/whs/directives/corres/pdf/850002p.pdf
25	DODD 8520.1	Protection of Sensitive Compartmented Information (SCI); http://www.dtic.mil/whs/directives/corres/pdf/852001p.pdf
26	DODD 8530.1	Computer Network Defense (CND); https://powhatan.iiie.disa.mil/cnd/dodd-o-8530-1.pdf
27	DODD 8530.1-M	Department of Defense Computer Network Defense (CND) Service Provider Certification and Accreditation Process; https://powhatan.iiie.disa.mil/cnd/dod-o-8530-1-m.pdf

28	DODD 8530.2	Support to Computer Network Defense (CND); http://www.dtic.mil/whs/directives/corres/html/853002.htm
29	DODD 8570.01	Information Assurance Training, Certification, and Workforce Management; http://www.dtic.mil/whs/directives/corres/pdf/857001p.pdf
30	DODD 8570.01-M	Information Assurance Workforce Improvement Program; http://www.dtic.mil/whs/directives/corres/pdf/857001m.pdf
31	DoDI 8510.01	DoD Information Assurance Certification and Accreditation Process (DIACAP) http://www.diacap.net/documents/851001p.pdf
32	DoDI 8500.2	Information Assurance (IA) Implementation http://www.diacap.net/Documents/DODI%2085002p-signed.pdf
33	FIPS 200	Minimum Security Requirements for Federal Information and Information Systems; http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf
34		Guidance Software Professional Development and Training EnCE Certification Program; http://www.guidancesoftware.com/training/EnCE_certification.aspx
35	HSPD-12	Homeland Security Presidential Directive 12, Policy for a Common Identification Standard for Federal Employees and Contractors
36	ICD Number 503	Intelligence Community Directive, Number 503, Intelligence Community Information Technology Systems Security Risk Management, Certification and Accreditation; http://www.dni.gov/electronic_reading_room/ICD_503.pdf
37		Information Assurance Risk Management Policy for National Security Systems; http://www.cnss.gov/Assets/pdf/CNSSP-22.pdf
38		Joint Air Force-Army-Navy (JAFAN) 6/9 Manual. Physical Security Standards for Special Access Program Facilities.
39		National Security Agency Security Configuration Guides; http://www.nsa.gov/snac/downloads_all.cfm
40		National Security Telecommunications and Information Systems Security Advisory/Information Memorandum (NSTISSAM TEMPEST), December 1995, Red/Black Installation Guidance (FOUO)
41	NIACAP	National Information Assurance Certification and Accreditation Process http://www.cnss.gov/Assets/pdf/nstissi_1000.pdf
42		NIST Publications Home Page; http://csrc.nist.gov/publications/index.html
43	NIST SP 800-61	Draft Computer Security Incident Handling Guide; http://csrc.nist.gov/publications/drafts/sp800-61-rev1/Draft-SP800-61rev1.pdf

44	NIST SP 800-48	Draft Wireless Network Security for IEEE 802.11a/b/g and Bluetooth; http://csrc.nist.gov/publications/drafts/800-48-rev1/Draft-SP800-48r1.pdf
45	NIST SP 800-80	Draft Guide to Developing Performance Metrics for Information Security; http://csrc.nist.gov/publications/drafts/draft-sp800-80-ipd.pdf
46	STIGS	All Applicable Security Technical Implementation Guidelines (STIGS)
47	TB 380-41	Technical Bulletin Security: Procedures for Safeguarding, Accounting and Supply Control of COMSEC Material.
48	Army CIO/G6 memo of 17 Aug 2010	Army Gold Master (AGM) Vista 9.X Compliance Guide https://chess.army.mil/ascp/commerce/scp/downloads/cb/AGM_Vista_%209X_Compliance_Guidance.pdf
49	Local Unit SOP	Applications and assigned networks standardization in look and feel.
50	Section 508	Section 508 Amendment to the Rehabilitation Act of 1973
51		Standardized COMSEC Custodian Course https://www.atrrs.army.mil/atrrscc/courseInfo.aspx?fy=2009&sch=757&crs=CATC-INT+34&crstitle=STANDARDIZED+COMSEC+CUSTODIAN+COURSE&phase=
52	AR 735-5	Policies and Procedures for Property Accountability (2005) http://armypubs.army.mil/epubs/pdf/r735_5_d20050228.pdf

2.18 Government Furnished Property, Services, and Equipment

2.18.1 Government Furnished Property (GFP) and Services. The Government will provide contractor personnel assigned to a site:

- Workspace including lights, ventilation, electric power, and facility maintenance/upkeep
- Facilities for contractor personnel within a reasonable distance of the equipment to be serviced
- Limited storage space for spare parts
- Police protection and physical security within the workspace
- Telephone service for mission related local and long distance calls
- Identification badges, security badges and vehicle passes/decals for access to the sites and controlled areas upon verification of security clearance
- Documentation for mission essential personnel to gain entrance to the site during crises as appropriate
- System/network access as appropriate

- Computer terminals and communications, as appropriate for sites serving as a remote service host location, access to secure work storage areas and secure communications to remote locations consistent with security requirements
- Access to the hardware host platform and access gateways for system diagnostics
- Parking is unique to each site and will be defined by the unit's ACOR

In the event the Government cannot provide the above GFP and services, the contractor may be required to provide them on a cost-reimbursable basis.

2.18.2 Government Furnished Equipment (GFE). All parts/spares owned by the Government and accountable under the c shall be identified and made accessible to the contractor. These parts shall be used to support the task order and repair actions initiated under the task order. The Government will be responsible for the transportation of GFE. Depending on availability, the Government may provide material handling equipment such as dollies, forklifts, hoists, or commercial-type vehicles. In the event the Government cannot provide transportation of GFE, the contractor may be required to transport GFE on a cost-reimbursable basis. The Government may train and/or license contractor employees to operate Government owned or leased equipment. The Government is responsible for disposal of all GFE. This responsibility cannot be delegated to contractor personnel.

2.18.3 Government Provided Services. The Government may provide contractor personnel assigned to a site the following:

- Space on military aircraft or other conveyance for the direct support of mission requirements
- Government shipment of approved equipment
- Communications devices for mission essential (unit designated) personnel

2.19 Contractor Equipment. The removal of contractor-owned equipment from the Government's facility is subject to DoD, Army, and IC security directives, regulations, and policies. The contractor's Transition Plan shall address the ingress and egress of this equipment in light of the Government's security restrictions.

2.20 Administrative Requirements

2.20.1 Government Shutdown Requirements for Mission Essential Contractor Personnel

2.20.1.1 Installation Closure. The installation commander may, at his discretion, close the post, installation or facility even if the Government is otherwise open. In this case (i.e., if the Government is open but the post, installation, or facility is closed) contractor personnel will not be able to report regardless of status. Unless the cognizant Government authority directs personnel to leave the installation, contractor personnel on site at the time of the closure may stay to complete their mission at the discretion of the contractor taking into account safety and other issues.

2.20.1.2 Alternate Duty Sites. In the case of either Government-wide or installation closure, the Contractor personnel whose place of duty is the installation or facility are not authorized to perform at an alternate duty site unless the task KO or COR/ACOR approves the type of work and the alternate location in writing in advance.

2.20.1.3 Notification. The COR/ACOR shall notify the contractor as to the instructions to be followed in the event of a Government shutdown. The contractor is responsible for the notification of its personnel.

2.20.1.4 Government Closure. In the event the U.S. Government Office of Personnel Management (OPM) officially announces closure of the Federal Government, and federal employees (other than emergency essential personnel) are not required to report to work, with the exception of Mission Essential Personnel. Personnel designated in writing by the COR/ACOR or verbally notified by the Contracting Officer (written confirmation will be provided within 2 business days) as mission essential shall report to work.

2.21 Familiarization Training. The Government may request the contractor familiarize Government personnel on new or upgraded hardware and/or software. A representative case where such support is required includes:

- System (hardware and software) maintenance for equipment that is to be deployed with Government personnel
- Installation of new software versions (e.g., operating system and office automation tools)

The Government will identify personnel to receive such instruction and approve the level of instruction recommended by the contractor. The instruction shall be conducted by resident contractor personnel at the central and/or remote site(s) and shall occur during the PPP.

2.22 Non-Disclosure. Prior to commencement of work, contractor personnel will be required to sign a Non-Disclosure Agreement (NDA). The successful contractor shall provide a list of executed NDAs with a self-certification within 15 days of task order award and annually thereafter to the COR/ACOR.

2.23 Contractor Support and Personnel Qualifications. The contractor shall develop, maintain and make available a current and accurate personnel database which records and tracks the qualifications, training, and security items necessary to meet the requirements of this PWS. The contractor shall provide sufficient qualified support at each unit (central site/remote locations) to ensure System Availability and TPRP compliance.

2.23.1 Technical Certifications. Contractor personnel supporting this effort must possess sufficient technical certifications, educational degrees, and experience to support the unit's unique requirements. Representative certifications include: CompTIA's A+, Network+, and Security+; Microsoft Certified Systems Engineer and Systems Administrator (with emphasis in Exchange); Cisco Certified Network Associate; and IT Infrastructure Library Certification, Representative software technologies implemented at the unit's include: Hypertext Markup and Extensible Markup Languages; Cascading Style Sheets; Active Server Pages; Java and JavaScript; Solarwinds Orion SL500; Microsoft Visual Basic, .Net, SQl Server, C#, Office,

Office Ultimate Suite, Server, System Center, Exchange, and DNS; Norton Antivirus; Blackberry Enterprise Server; Lumension Sanctuary, Hercules and Host Based Security System; MacAfee; Remedy, VERITAS; and Oracle databases. Contractor personnel performing equipment repair shall possess OEM certification and shall maintain currency on OEM equipment and complete training to receive manufacture's certification to repair equipment. Contractors must be trained and certified in accordance with DoD 8570 series directives and regulations prior to starting work at a site.

2.23.2 Hazardous Material Training. Contractor personnel supporting this effort shall be trained for Hazardous Material (HAZMAT) requirements relevant to the work assigned. Contractor personnel supporting this effort shall possess all state and local licenses required for the performance of specific duties outlined in this PWS.

2.23.3 Government Mandatory Training. All contractors performing work on site must complete government directed mandatory training.

2.24 OCONUS Contractor Conduct and Appearance. Personnel participating in and providing support to military training exercises, regular or Quick Reaction Capability (QRC) deployments, contingency operations, hostilities, war, or other unusual situations may be required to wear Nuclear Biological Chemical/Chemical Biological Radiological (NBC/CBR) protective clothing/masks, attend training applicable to the effort, receive inoculations, and utilize supporting equipment when required by the supported Commander and directed by the COR or Administrative COR (ACOR), if appropriate. When required by the Mission or Theater Commander, the Government will provide to the contractor all military unique individual equipment. Personnel who display disruptive behavior or violate substance abuse laws or regulations of host nations or host military commanders shall be immediately terminated from the program and returned to CONUS at contractor expense. The contractor shall be responsible for ensuring the employees assigned to this contract comply with the applicable laws and regulations of the host country and any political subdivisions thereof. The contractor is also responsible for ensuring the employees comply with military rules and regulations when employed in areas under the jurisdiction of the applicable U.S. Army Commander. In the event a contractor's employee is banned from continuing to perform under the contract for failure to, comply with the laws, rules, and regulations, the costs incurred by the contractor because of the removal of the employee or the substitution of a replacement employee shall not be reimbursable under this contract. The disallowed costs would include relocation costs incurred by the contractor to furnish a suitable substitute employee for the overseas assignment. Loss or suspension of required security clearance as set forth on the DD Form 254, "Contract Security Classification Specifications," would result in the contractor's inability to perform in accordance with the terms and conditions of this contract. As a result of this failure to perform, the contractor is subject to termination under the appropriate termination clause herein.

2.25 Material Purchases. In the event the contractor requires replacement parts and components to support C4IM Systems, purchases will be placed through the Computer Hardware, Enterprise Software and Solutions contracts to the maximum extent possible. Procurements will be cost reimbursable.

2.26 Overtime. The Government may approve overtime to support the mission of the unit supported. Overtime must be requested in advance and approved by the KO or their authorized representative (COR or the site ACOR).

2.27 Insurance. Upon task order award and in accordance with FAR clause 52.228-7, Insurance – Liability to Third Persons, the contractor shall certify to the KO, prior to commencing work that he has and will maintain, without interruption throughout the performance of the task order, the types of insurance for minimum amounts of coverage set forth in the contractor's base contract.

2.28 Incentives. TBD

2.29 Contracting Officer's Representative (COR):

2.29.1 The COR will be identified at award:

HQ, INSCOM, Directorate of Contracting
COR:
8825 Beulah Street,
Fort Belvoir, VA 22060-5246

2.29.2 COR/ACOR monitors all technical aspects of the contract and assists in contract administration. A letter of COR/ACOR designation is issued to the COR/ACOR with a copy of which is sent to the contractor, stating the responsibilities and limitations of the COR/ACOR, especially with regard to changes in cost or price, estimates or changes in delivery dates. The COR/ACOR is not authorized to change any of the terms and conditions of the resulting order.

3.0 DELIVERABLES

Unless otherwise noted, all deliverables will be provided to the COR, ACOR and the KO. Delivery will be one (1) hard copy to the COR and electronically to the KO and ACOR. Format will be as proposed by the contractor and approved by the Government.

TABLE 2 - DELIVERABLE ITEMS AND SCHEDULE

Deliverable Items and Schedule				
Deliverable	**Frequency**	**# of Copies**	**Medium/Format**	**Submit To**
System Status	Daily	TBD	Electronic/Hard Copy (MS Word)	CIO/G6 Mgmt Staff
System Update Notice	As Required	1	Electronic/Hard Copy (MS Word)	COR/ACOR
Operations Status	Weekly	1	Electronic/Hard Copy (MS Word)	COR/ACOR
Change Management Status	Weekly	1	Electronic/Hard Copy (MS Word)	COR/ACOR

CM Action Items	As Required	1	Electronic/Hard Copy (MS Word)	COR/ACOR
IA Data and Documentation	As Required	1	Electronic/Hard Copy (MS Word)	COR/ACOR
ASID	As Required	1	Electronic/Hard Copy (MS Word)	COR/ACOR
Contractor's Bi-Annual Customer Survey Plan	Ten (10) business days prior to survey	1	Electronic/Hard Copy (MS Word)	COR/ACOR
Bi-Annual Customer Survey Results and Contractor Improvement Report	Thirty (30) days after Survey Completion	1	Electronic/Hard Copy (MS Word)	COR/ACOR
Staffing List	As Required	1	Electronic/Hard Copy (MS Word)	COR/ACOR
Unit Transition Plan	Sixty (60) days prior to the expiration of a performance period	1	Electronic/Hard Copy (MS Word)	COR/ACOR
Monthly Status Reports	Monthly (by 15th of month)	1	Electronic/Hard Copy (MS Word)	COR/ACOR

The Contractor shall provide the following deliverables:

3.1 Deliverable **Documentation.** Government personnel will review the materials presented and evaluate them for accuracy and completeness. The Government will notify the contractor of deliverable acceptance within five (5) working days of receipt of the deliverable. All days in proposed schedules are calendar days unless otherwise stated. Each deliverable will be provided to the COR/ACOR.

3.2 System Status. Contractor shall provide data and information on the availability of the IT System and status of all update, repair and remedial maintenance activities.

3.3. System Update Notice. Contractor shall provide reasons and description of the proposed update, the contractor's plan of action and the contractor's impact assessment.

3.4 Operations Status. Contractor shall provide data and information on the status of planned and on-going IT System operation activities.

3.5 Change Management Status. Data and information on the status of all open change management actions.

3.6 CM Action Items. Contractor shall provide reports, white-papers, briefings, and other documentation as specified by CM Board or unit's business processes.

3.7 IA Data and Documentation. Contractor shall provide data and documentation to support the unit's IA IAVM and FISMA responsibilities.

3.8 ASID. Contractor shall provide ASID maintenance reports (which include inventory results).

3.9 Contractor's Bi-Annual Customer Survey Plan. Contractor shall provide Contractor's plan for conducting the survey to include specifics on the who, what, when and how the survey will be conducted, together with how the results will be reported.

3.10 Bi-Annual Customer Survey Results and Contractor Improvement Report. Contractor shall provide data and information with Contractor's proposed improvements, based upon the customer survey results **3.5 Staffing Report.** Contractor shall provide a monthly staffing report to the COR/ACOR or as changes dictate.

3.11 Staffing List. Contractor shall provide identification of all contractors, by name, providing support on task order(s). Final format to be specified by the COR/ACOR.

3.12 Unit Transition Plan. Contractor shall provide a plan to phase in or out the units CIO/G6 ENTERPRISE task order.

3.13 Monthly Status Reports. Contractor shall provide the status of Technical Performance and Financial Data, final format to be specified by COR/ACOR.

3.14 Engineering Deliverables

U. S. Government contractors should contact their COR/ACOR for distribution of these documents. Publications available on-line can be accessed at the following web sites:

http://www.weibull.com/knowledge/milhdbk.htm
http://www.product-life-cycle-management.com/legacy-military-standards.htm
http://www.apd.army.mil
http://members.asme.org/catalog/CategoryView.cfm

ASME-Y14.38M	Abbreviations for use on Drawings
MIL-STD-100G Sep 97	Engineering Drawing Practices
MIL-T-31000C Jul 04	Technical Data Packages
MIL-HDBK-61A(SE)	Configuration Management

Sep 97	
DOD-STD-480B Jul 88	Configuration Control
MIL-STD-1285B Sep 04	Marking of Electronic Parts
ANSI-Y14.5M	Dimensioning and Tolerancing