A Statement of Work (SOW) is typically used when the task is well-known and can be described in specific terms. Statement of Objective (SOO) and Performance Work Statement (PWS) emphasize performance-based concepts such as desired service outcomes and performance standards. Whereas PWS/SOO's establish high-level outcomes and objectives for performance and PWS's emphasize outcomes, desired results and objectives at a more detailed and measurable level, SOW's provide explicit statements of work direction for the contractor to follow. However, SOW's can also be found to contain references to desired performance outcomes, performance standards, and metrics, which is a preferred approach.

The Table of Content below is informational only and is provided to you for purposes of outlining the PWS/SOO/SOW. This sample is not all inclusive, therefore the reader is cautioned to use professional judgment and include agency specific references to their own PWS/SOO/SOW.

STATEMENT OF WORK

Project Name & ID: _____

May 1, 2011

1.0 SCOPE

The contractor shall provide all personnel and other items and non-personal services necessary to perform xxx Headquarters enterprise-level Command, control, communications, computer, and information technology support as defined in this Performance Work Statement except as specified in Part 3 as Government Furnished Property (GFP). The contractor shall perform to the standards in this PWS. The contractor shall provide engineers, technicians, software developers, and specialists on-site and on-call to administer xxx systems and networks. The contractor shall integrate any technology changes and upgrades as approved by the Contracting Officer to meet user requirements and to maintain operational currency of Information Technology/Information Management (IT/IM) systems and networks. Currently, the Headquarters xxx is composed of approximately xxx users distributed amongst a campus environment. By 2010, it is expected to increase to xxx users.

The contractor shall attend program meetings such as status meetings, Project Control Boards, program reviews, Configuration Control Boards (CCB), and other sustainment activities. The contractor shall be prepared to answer questions pertaining to sustainment of xxx IT/IM systems and networks, and present the results of research completed to the Contracting Officer Representative (COR).

The following tasks apply to this PWS: Technology Insertion, Systems Integration and Systems Engineering; Installation, Hardware and Software Fabrication, Test and Evaluation, Certification, Studies and Analyses, and Technical Data Management.

1.1 GENERAL

1.1.1 DESCRIPTION OF SERVICES/INTRODUCTION

1.1.2 BACKGROUND

1.1.3 OBJECTIVES

The contractor shall establish a program of support for the xx to provide effective enterprise-level Command, control, communications, computer, and information technology capabilities, which provide the Government resources needed to achieve the four-star Combatant Command's (COCOM) operational objectives.

1.2 APPLICABILITY

The following tasks apply to this SOW: Technology Insertion, Systems Integration and Systems Engineering; Installation, Hardware and Software Fabrication, Test and Evaluation, Certification, Studies and Analyses, Technical Data Management, Logistics Support, and Training.

1.3 TASK PROPOSAL

The contractor shall provide a Task Proposal in response to this task order. The effort shall be proposed on a **Time and Materials (T&M)** basis.

1.4 PERIOD OF PERFORMANCE / PLACE OF PERFORMANCE

The period of performance shall be 12 months from date of award with two (2) twelve (12) month option periods.

The Government will allow a ten (10) working day transition immediately following the initial task order award, as security clearances are settled and staff are brought on-line. The Contractor will be required to submit a transition plan within two (2) work days of the contract start date. If the incumbent wins this will not apply.

xxx Headquarterss, a Government-provided facility located at xxx

1.5 CONTRACT MANAGEMENT

The Contractor shall submit a monthly Contractor's Progress, Status and Management Report required by DI-MGMT-80227 and CDRL A002. For this task order, the Contractor shall discuss the following:

- Significant accomplishments and issues that arose during the reporting period.
- Projected activities for the following and subsequent periods.
- Subcontractor performance, as applicable.
- Any meetings held with government representatives, as applicable.
- Performance to the metrics established in the approved proposal.

For this Time and Materials task, the Contractor shall report the following cost data:

- Expenditures for the reporting period, by Labor, Materials and ODCs. (Labor costs shall be broken down by labor category, entity, such as prime or subcontractor, rate and hours. Materials costs and ODCs shall be identified and discussed).
- Total task expenditures for the fiscal year to date, indicated as total, labor, materials and ODCs.
- Total task expenditures since task award, indicated as total, labor, materials and ODCs.
- Remaining funds, monthly burn rate, and projected burn rate until task completion

1.6 GOVERNMENT FURNISHED EQUIPMENT / MATERIALS / FACILITIES / INFORMATION

The government shall provide, the facilities, equipment, materials, and/or services listed below.

1.6.1 EQUIPMENT

The government will provide telephones, computer equipment (to include all necessary hardware & software), and associated peripheral devices, facsimile machines, copier, and other basic office supplies required to complete the task described in the PWS. The Government will issue user identification and passwords to Government networks IAW established procedures.

1.6.2

All Government Furnished Equipment (GFE) will be identified and transferred to the contractor as required for support of the applicable IT/IM systems and networks. The contractor will receive a copy of the GFE hand receipt report upon award of the Task Order (TO) as requested. All GFE shall be returned to the Government at Task Order completion.

1.6.3 DISPOSITION OF REPLACED / UNSERVICEABLE PARTS:

Any parts, components or assets that are made available by replacement, repair, upgrade, or reconfiguration during the performance of this task, shall remain the property of the Government.

1.6.4 UTILITIES:

All utilities in the facility will be available for the contractor's use in performance of duties outlined in this PWS. The Contractor shall instruct employees in utilities conservation practices. The contractor shall be responsible for operating under conditions that preclude the waste of utilities.

1.6.5 FACILITIES:

The Government will furnish the necessary workspace for the contractor staff to provide the support outlined in this PWS.

1.6.6 INFORMATION:

The Government will furnish engineering drawings, interconnection diagrams, circuit diagrams, and floor plans. The Government will issue user identification and passwords to Government networks IAW established procedures. The Government will provide any software design documents, access to source code and libraries, and previously developed training software (Computer-based training, or web-based training packages) and all Powerpoint and paper-based materials, such as manuals.

1.7 INSPECTION AND ACCEPTANCE

Inspection and acceptance shall be at xxxxx

1.7.1 SCOPE OF INSPECTION:

All deliverables will be inspected for content, completeness, accuracy and conformance to Task Order requirements by the COR. Inspection may include validation of information or software through the use of automated tools and/or testing of the deliverables, as specified in the Task Order. The scope and nature of this testing must be negotiated prior to Task Order award and will be sufficiently comprehensive to ensure the completeness, quality and adequacy of all deliverables.

The Government requires a period not to exceed fifteen (15) work days after receipt of final deliverable items for inspection and acceptance or rejection.

1.7.2 BASIS OF ACCEPTANCE:

(For all CLINs) The basis for inspection/acceptance shall be compliance with the requirements set forth in the Task Order, the contractor's proposal and other terms and conditions of the contract including the Government Quality Assurance Surveillance Plan (QASP)/Quality Control Plan (QCP). Deliverable items rejected shall be corrected in accordance with the applicable clauses.

Reports, documents and narrative type deliverables will be accepted when all discrepancies, errors or other deficiencies identified in writing by the Government have been corrected.

If the draft deliverable is adequate, the Government may accept the draft and provide comments for incorporation into the final version.

All of the Government's comments to deliverables must either be incorporated in the succeeding version of the deliverable or the contractor must demonstrate to the Government's satisfaction why such comments should not be incorporated.

If the Government finds that a draft or final deliverable contains spelling errors, grammatical errors, improper format, or otherwise does not conform to the requirements stated within this Task Order, the document may be immediately rejected without further review and returned to the contractor for correction and resubmission. If the

contractor requires additional Government guidance to produce an acceptable draft, the contractor shall arrange a meeting with the ALTESS COR.

1.7.3 WRITTEN ACCEPTANCE/REJECTION BY THE GOVERNMENT:

The Government shall provide written notification of acceptance or rejection of all final deliverables within fifteen (15) work days. All notifications of rejection will be accompanied with an explanation of the specific deficiencies causing the rejection.

1.7.4 NON-CONFORMING PRODUCTS OR SERVICES:

Non-conforming products or services will be rejected. Deficiencies will be corrected, by the contractor, within ten (10) work days of the rejection notice. If the deficiencies cannot be corrected within ten (10) work days, the contractor will immediately notify the ALTESS TR of the reason for the delay and provide a proposed corrective action plan within ten (10) work days.

1.8 SECURITY

1.8.1 SECURITY REQUIREMENTS:

The security requirements for this task are defined in the DD254. The contractor facility security officer (FSO) shall provide a transition plan for contractors to obtain their security badges through xxx Headquarters security office.

1.8.2 SECURITY CLEARANCES:

The contractor shall safeguard all government property provided for contractor use. The contractor shall ensure that the government facilities, equipment and materials are secured at the close of each work period.

The highest level of security clearance requirement for this Task Order is Top Secret (TS) with Sensitive Compartmented Information (SCI) access of sensitive information/talent keyhole (SI/TK). Personnel must possess a Top Secret/Sensitive Compartmented Information (TS/SCI) security clearance or be able to be granted an interim clearance within 60 days of hiring date. In addition, those positions with a TS or higher clearance level are subject to testing for illegal drug use. The contractor shall follow DoD Federal Acquisition Regulation Supplement (DFARS) clause 252.223-7004, Drug-free Work Force; and local policies regarding drug testing. The contractor shall perform drug tests, ensuring all TS-cleared contractor employees are tested at least once a year, every year of the TO, as well as when there is a reasonable suspicion that a employee uses illegal drugs, at the contractor's expense. Any positive test result shall be made available to the COR immediately. Records of drug testing shall be made available to the COR upon request.

The contractor shall take appropriate measures to safeguard their Government issued security badges and common access cards (CAC) as outline in HQ's security policies and other applicable regulations.

The contractor will require access to xxx information; Sensitive Compartmented Information (SCI); NON-SCI intelligence information; NATO information; and For Official Use Only (FOUO) information. The contractor will require access to the SIPRNET system.

Administrative duties performed by the contractor will not require a clearance but may require an investigation for Information Technology (IT) sensitive duties.

1.8.3 FACILITY CLEARANCE:

The contractor shall maintain a TOP SECRET facility clearance with NO safeguarding requirements.

1.8.4 CLASSIFIED MATERIAL:

The contractor shall properly safeguard all classified material in accordance with applicable regulations outlined in the DD Form 254.

1.8.5 PHYSICAL SECURITY:

The contractor shall take appropriate Government-prescribed security measures to ensure systems and other Government property is stored and installed in accordance with security guidelines and applicable regulations. The contractor shall notify the Government any time the contractor moves Government, or Government Furnished, Equipment (GFE) .

1.8.6 LOCK COMBINATIONS, USER ACCOUNTS, AND PASSWORDS:

The Contractor shall establish and implement methods of ensuring that all lock combinations and passwords are not revealed to unauthorized persons. The Contractor shall ensure that lock combinations are changed when personnel having access to the combinations no longer have a need to know such combinations. The contractor shall ensure that IT user and administrator passwords are changed in accordance with DOD Policy. Contractor shall delete user network accounts as users no longer have a need to access the xxxx accredited networks. These procedures shall be included in the Contractor's Quality Control Plan.

1.8.7 CONSERVATION OF UTILITIES:

The contractor shall instruct employees in utilities conservation practices. The contractor shall be responsible for operating under conditions that preclude the waste of utilities. The contractor shall ensure all employees have a valid driver license and completed the vehicle

1.8.8 SPECIAL QUALIFICATIONS:

The contractor shall ensure that all employees have a valid driver license and have completed the vehicle driving accident avoidance course required to operate a GSA vehicle.

1.8.9 POST AWARD CONFERENCE/PERIODIC PROGRESS MEETINGS:

The Contractor shall attend any post award conference convened by the contracting activity or contract administration office in accordance with Federal Acquisition Regulation Subpart 42.5. The Contracting Officer (KO), Contracting Officers Representative (COR), and other Government personnel, as appropriate, may meet periodically with the contractor to review the contractor's performance. At these meetings the Contracting Officer Representative will apprise the contractor of how the government views the contractor's performance and the contractor will apprise the Government of problems, if any, being experienced. Appropriate action shall be taken to resolve outstanding issues.

1.8.10 CONTRACTING OFFICER REPRESENTATIVE (COR):

The (COR) is identified below:

The COR monitors all technical aspects of the contract and assists in contract administration. The COR is authorized to perform the following functions: assure that the Contractor performs the technical requirements of the contract: perform inspections necessary in connection with contract performance: maintain written and oral communications with the Contractor concerning technical aspects of the contract: issue written interpretations of technical requirements, including Government drawings, designs, specifications: monitor Contractor's performance and notifies both the Contracting Officer and Contractor of any deficiencies; coordinate availability of government furnished property, and provide site entry of Contractor personnel. A letter of designation issued to the COR, a copy of which is sent to the Contractor, states the responsibilities and limitations of the COR, especially with regard to changes in cost or price, estimates or changes in delivery dates. The COR is not authorized to change any of the terms and conditions of the resulting order.

1.8.11. PROGRAM MANAGER/CONTRACT MANAGER:

The contractor shall provide a contract manager who shall be responsible for the performance of the work. The name of this person and an alternate who shall act for the contractor when the manager is absent shall be designated in writing to the contracting officer. The contract manager or alternate shall have full authority to act for the contractor on all contract matters relating to daily operation of this contract.

1.8.12. IDENTIFICATION OF CONTRACTOR EMPLOYEES:

All contract personnel attending meetings, answering Government telephones, and working in other situations where their contractor status is not obvious to third parties are required to identify themselves as such to avoid creating an impression in the minds of members of the public that they are Government officials. In addition all documents or reports produced by contractors are suitably marked as contractor products or that contractor participation is appropriately disclosed. Contractor personnel shall obtain and wear Government issued Common Access Card (CAC) and/or Government facility badges provided at assigned posts.

1.8.13. KEY PERSONNEL:

The contractor shall assign and identify an on-site contract manager to provide management and administrative and technical interaction with Government members in the day-to-day accomplishment of support services. The contractor shall designate and identify contractor employees who will be considered key to operations for efforts under this task order. These key personnel must have an in-depth understanding of the requirements and their responsibilities as well as the ability, knowledge, experience, and skills to perform the requirements. They shall be fully committed to the success of the mission. During bad weather, the ASA is required to support the emergency command center. The contractor shall designate key personnel for the following tasks:

Computer Systems Analyst
Help Desk
Information Assurance
Network Management
System Administration
Technical Control Facility
Telecommunications Specialist

2.0 APPLICABLE DOCUMENTS

The following documents are referenced for the performance of this effort:

The PWS may set a higher standard of performance than an applicable Army regulation. The PWS will control over the regulations unless a particular provision is in direct conflict with the applicable provision of the Army regulation. The Contracting Officer (KO) will make this determination. Most publications may be downloaded from the Internet Web sites or may be ordered. The Government will provide those publications not available on a Web site or via mail order. The contractor shall inform the COR of any change to a publication or document that affects the cost of the Task Order.

Department of Defense (DOD):

DOD 5220.22-M, National Industrial Security Program, Operating Manual,
28 February 2006.
DOD CIO Memo, Interim Department of Defense (DOD) Information Assurance (IA) Certification and Accreditation (C&A) Process Guidance, 6 July 2006.
DIACAP Frequently Asked Questions (FAQs), 18 July 2006.
DODD 5230.24, Distribution Statements on Technical Documents,
18 March 1987.
DOD 8510.01 DOD Information Assurance and Accreditation Process,

28 November 2007.
DoDD 8500.1, Information Assurance, 24 Oct 2002.
DODI 8500.2, Information Assurance (IA) Implementation, 6 Feb 2003.
DOD 8570.01-M, Information Assurance Workforce Improvement Program, Dec 2005.
DoDI 8580.1, Information Assurance in the Defense Acquisition System, 9 July 2004.
SIPRNET GIG Interconnection Approval Process (GIAP) Cross Domain Solution (CDS) Connection Requirements, July 2004.
NSTISSI No.7003, Protective Distribution Systems (PDS), 13 Dec 1996.
NSTISSAM TEMPEST/2-95A, Red/Black Installation Guidance, Amendment, 3 February 2000.
CJCSI 6510.06 (Series): "Communications Security Release to Foreign Nations."

Regulation, Federal:
Presidential Decision Directive PDD-63 Critical Infrastructure Protection
E-Government Act of 2002 (Public Law 107-347).
Federal Information Security Management Act of 2002 (Title III of E-Gov).
NSA/CSS Policy Manual 3-16: "Control of Communications Security (COMSEC) Material."

3.0 REQUIREMENTS

3.1 SYSTEMS ADMINISTRATION

The Government Active Directory network is comprised of approximately 200 Windows 2002/2003 and LINUX servers. The network of record for day-to-day operations is the Secure Internet Protocol Routing Network (SIPRNET); therefore, it holds approximately two-thirds of the 200 servers. However, the majority of the users have both a SIPRNET and a Non-classified (but Sensitive) Internet Protocol Routing Network (NIPRNET) client under their desk. File servers and MS Exchange servers are clustered to provide redundancy and high availability. Refer to Appendixes 3 and 8 for a list of the servers, functions, and software.

The contractor shall:

3.1.1

Provide system administration for all IT/IM systems and networks, on-site during the hours required within this PWS. Additionally, the contractor shall provide Microsoft (MS) Windows system administrator staff to support the requirement that a MS Windows systems administrator be on-call 24 hours a day, 7 days a week (24x7).

3.1.2

Maintain the LANs, systems, and local procedures in accordance with Department of Defense (DoD), regulatory guidance and doctrine and, when applicable, with the International Standards Organization (ISO) recommendations. Contractor shall include all events of LAN outages in monthly reports to the Government. The contractor shall maintain a 98% network availability on this order. The contractor shall provide to the COR a monthly report of the service level and appropriate calculations in accordance with CDRL B001.

3.1.3

Manage all servers; perform log analysis, error detection, fault correction, backups, and restores; perform startup and shutdown of the systems as required and with prior Government coordination; and build, configure, patch, and upgrade servers, operating systems, and server applications as required and with prior COR coordination following the security technical information guidance (STIG).

3.1.4

Maintain daily, weekly, and monthly scheduled network backups; restore data as required to support systems and data recovery due to hardware, software, or user error; verify and validate the integrity of the backups; and perform recovery test or drills periodically in coordination with COR guidance. The current backup configuration for the networked servers and data is composed of Comm Vault Galaxy Software backing up to an ADIC IScaler 2000 on both the SIPRNET and the NIPRNET, and DELL Power Vault 128T at the satellite sites. Current backups are conducted on a daily basis (incremental), with full backups performed on weekends. All other information assurance appliances, systems, network and their appropriate IOS/OS's will be backed up to ensure proper and expedient service restoral in the event of a system outage. Level of Service for backups and data restoration is 99%.

3.1.5

Perform email administration and postmaster duties and functions, to include internal Dynamic Domain Name Service (DDNS) support, directory synchronization, Simple Mail Transfer Protocol (SMTP) gateway administration, and email management; manage the Global Address List (GAL) on the MS Exchange server; and develop and manage distribution lists and interface to other MS Exchange networks. Currently, six MS Exchange clustered email servers provide failover support to approximately 5,000 mailboxes. Two email servers are on the NIPRNET (2,500 mailboxes) and four on the SIPRNET (2,500 mailboxes). In both cases, the email databases reside in the storage area network (DELL/EMC CX600). The Government runs Enterprise Vault on the SIPRNET, where all 30-day email is archived. The NIPRNET vaulting is performed using COMVAULT. The contractor shall implement COMVAULT on the SIPRNET so as to standardize. Government will provide the hardware and software. SympleSynch provides email global address list synchronization with the networks in the area of focus (AOF). The Government Agency acts as the "hub" for the Light Directory Access Protocol (LDAP) synchronization configuration. MS DDNS is implemented on the internal network to support the Active Directory domain. A Defense Information Infrastructure (DII) Mail Guard connects both SIPRNET and NIPRNET LANs and provides high-to-low and low-to-high email support for our customers. Contractor shall serve as an expert for the Automated Message Handling System (AMHS) and the Defense Messaging System (DMS).

3.1.6

Collaborative tools are based on Government's IBM Sametime implementation. Its sessions and accounts are based on DISA's services, while the Agency provides the client-level support. The contractor shall facilitate and provide support to customers on IBM Sametime client issues.

3.1.7

Scripting Management: The contractor shall ensure that repetitive processes are automated to ensure efficiencies and effective handling of tasks. To this effect the contractor shall implement Commercial Off the Shelf (COTS) applications as applicable and approved by the COR or develop scripts. Examples of scripting tasks include the automation of the account-creation process, renaming of a wide range of accounts to another naming convention, and automatic notification to users on account statuses based on "triggers." Specifics on what may be required are subject to changes in Government guidance, Agency directives, upgrades, migrations, etc.

3.1.8

Manage, operate, and support the secure and non-secure Virtual Private Network (VPN) access and gateways. The contractor shall support user-access requirements.

3.1.9

Control and monitor user access to the LANs. The contractor shall add, delete, and modify user access to the network resources; manage account profiles, permissions, and access to resources; and create accounts within 24 hours of account request submission. The directorates' information technology officers (ITOs) submit account requests on-line via the Agency SIPRNET portal. Upon receipt of an account request, a system administrator builds the network and email accounts for the SIPRNET and NIPRNET. The user picks up and signs for the accounts at

the help desk. The contractor shall monitor, disable, and remove inactive accounts as well as control permissions. NOTE: The Agency uses roaming profiles on this network in order that the users may move from client to client. The contractor shall create and recreate profiles as necessary.

3.1.10

Support the connectivity of other systems to the networks and troubleshoot connectivity problems.

3.1.11

Test and integrate all IT/IM modifications and upgrades to ensure compatibility with and integrity of the network.

3.1.12

Maintain and monitor system resource utilization, such as disk configuration, memory, and central processing unit (CPU), on servers, routers, switches, and desktops; recommend changes and make those that are approved by the COR; and perform desktop analysis at the time of developing the baseline or when troubleshooting.

3.1.13

Assess and identify network deficiencies, recommend corrective action, and engineer and integrate said recommendations as tasked by the COR. The Contractor shall provide shall recommendations and documentation in a Scientific and Technical Report in accordance with Contracts Data Requirement List (CDRL).

3.1.14

Notify the Government immediately of any problems that occur during daily maintenance of servers, switches, routers, etc. Examples are problems accomplishing backups, disk-space utilization, and excessive CPU utilization.

3.1.15

Maintain system evaluations and certifications as required; e.g., system security authorization agreements, certifications to operate, and other system certifications.

3.1.16

Provide technical advice and support to the Communications Team, focused on mobile communications support and automation expertise for the mobile team and the Command Group traveling staff. Please note: Contractor travel is not required in support of this requirement.

3.1.17

Implement patch management of the networks as tasked and suspended by the Government. Findings and mitigations shall be addressed in accordance to the Agency or local policies.

3.2 INFORMATION ASSURANCE SUPPORT

3.2.1

Support antivirus software updates and apply the definitions to the network servers and workstations.

3.2.2

Support security incident reporting on all network computer security incidents and spillages. The contractor shall submit a Scientitic and Technical Report IAW with Contracts Data Requirement List (CDRL).

3.2.3

Review and support all incoming information technology requests (ITR).

3.2.4

Support vulnerability assessments in accordance with authority directives; perform information assurance vulnerability alert (IAVA) compliance scans against the servers and workstations on both the SIPRNET and NIPRNET networks; scan the networks to perform vulnerability assessments; and install the latest releases and updates for the Retina client software or appropriate scanning tools.

3.2.5

Reply to and take action on all communications tasking orders (CTO) that require Government input. Contractor shall obtain Government approval on CTOs.

3.2.6

Review and store the systems, security, and application event logs from servers. Review and store network event logs.

3.2.7

Provide patch management support; maintain the networks' security posture by implementing and managing the Information Assurance Vulnerability Management (IAVM) process, complying with Government directives.

3.2.8

Information Assurance

3.2.8.1

Support the Information Assurance Manager (IAM): Implement security policies and procedures for the overall security management of Automated Information Systems (AISs). Oversees the entire security program and ensures the security plan is adhered to. Oversee the Information Assurance Program and ensure the security posture of the HQ's network is maintained to the highest standards. Coordinate with the System Administrators concerning AIS security issues. Maintain security procedures for all AISs and networks, in accordance with Regulation 1001 and local operating instructions. Responsible for ensuring all System Administrators (SA) and security staff are appointed in writing. Review the audit logs with the SAs for anomalies. Administer all AIS security matter for the command. Conduct and document risk and self-assessments at least annually. Prepare and maintain plans, instructions, guidance and Standard Operating Procedures (SOPs) regarding the security of automated operations and distribute to system users and submit for COR/Government approval. Prepare and assist for the annual audit (Evaluation Compliance Visit (ECV).

Oversee the implementation of appropriate countermeasures. Implement and oversee the implementation of the Security Awareness, Training and Education (SATE) Program. Ensure System Administrators evaluate, report, and document all security problems and vulnerabilities discovered. Prepare and maintain all System Security Authorization Agreements (SSAA's) and ensure suspenses are met.

3.2.8.2

Implement and manage a wide range of network security systems, to include firewalls, intrusion prevention systems (IPS), mail filters, vulnerability management system (VMS), Host Base Security System (HBSS), intrusion detection systems (IDS), RETINA scanning software, Anomaly Detection System (ADS), Retina Enterprise Management (REM), and the information assurance management systems (IAMS).

3.2.8.3

Support firewall administration; build, configure, implement, and monitor the SIPRNET and NIPRNET network firewalls; configure the rules, monitoring and troubleshooting the network traffic traversing through the firewall.
3.2.8.4

Support IPS (network and servers): Monitor server performance and ensure all application services are running; maintain and backup the IPS SQL database; correlate the IPS output with the firewall and server logs to determine if any intrusion has occurred; review the server sensor output to the IPS console for suspicious activity on the servers and take appropriate action in accordance with regulatory guidelines; maintain the network keys; and configure the IPS security policy for network sensor and/or server sensors to monitor malicious activity reported.

3.2.8.5

Support Web content filters, and monitor and control access to prohibited Web sites in accordance with regulatory guidance.

3.2.8.6

Support email filter administration; validate emails sent to the spam mailbox and forward official blocked emails to the customer; and monitor the filtered emails in the mail repository in accordance with established standard operating procedures (SOP) to eradicate spam emails.

3.2.8.7

Support antivirus software updates; manage the antivirus software by monitoring the CERT Web site at least twice a day for newly released definition updates and applying the definitions to the network servers and workstations.

3.2.8.8

Monitor the workstations for Spyware and Adware using Spyware and Adware tools and applications.

3.2.8.9

Support security incident reporting; collect and gather information pertaining to network computer security incidents and spillages; and create the initial, follow-up, and final report pertaining to each incident. The contractor shall brief the ASA security manager and forward the report to the COR, IAW Contracts Data Requirement List.

3.2.8.10

Review and update the system password logs and notify system administrators of any changes required.

3.2.8.11

Review and store the systems, security, and application event logs from servers. Review and store network event logs.

3.2.8.12

The contractor shall operate, maintain, manage, configure, troubleshoot, and install the following software and any additional software that may be added or changed:

McAfee Mail Security and Spam Filter
Sidewinder Firewall
McAfee Antivirus /antispyware

DISA Gold Disk utility
Retna Scans MS Windows XP/2003 Server
Site Protector
Snort - Red Hat Linux
Websense Web Filter
Anomaly Detection Systems
Mobile Armor - Data at Rest
Device Lock
CS-Mars
Microsoft ISA Servers

3.2.8.13

The contractor shall operate, maintain, manage, configure, troubleshoot, and install the following software and any additional hardware platforms that may be added or changed:

DELL Blades servers: IPS
DELL server: SNORT IDS site protector
Sidewinder: firewall appliance
DELL server: Real Secure
Iron Mail: filter appliance
DELL server: site protector
DELL server: Retna scans

3.3 DATABASE MANAGEMENT AND ADMINISTRATION

The contractor shall function as the database manager and administrator of the Agency LANs. The contractor shall perform the following functions, but not limited to, in an MS SQL environment:

3.3.1

Maintain the existing common-user MS SQL databases resident on LAN servers and design, structure, and maintain additional databases as required supporting new applications.

3.3.2

Add, delete, and modify user access and permissions to common-user databases (resident on LAN servers) as required.

3.3.3

Schedule and perform daily database backups and perform database recoveries as required. The contractor shall be responsible for the integrity of the data in all databases under their responsibility.

3.3.4

Develop MS SQL databases to support business processes and functions or to support Web applications.

3.4 WEB AND APPLICATION DEVELOPMENT

The contractor shall:

3.4.1

Develop and maintain new and existing computer-based training (CBT) modules in support of the sustainment base training requirements and the Agency unique program requirements utilizing Macromedia’s Authorware. The

contractor shall support approximately 12 existing Authorware-developed Computer Based Training (CBTs) modules.

3.4.2

Analyze, identify, design, and integrate unique solutions to sustain and improve user business processes; perform scripting and support and automate network processes as necessary.

3.4.3

Develop and maintain new and existing local unique applications in support of Agencwork-process improvement and business processes; use a combination of MS .NET, Visual Basic, and Crystal Reports on an Internet Information Services (IIS) and SharePoint platform to develop said applications; and currently support (operate, maintain, manage, configure, troubleshoot, and install) approximately 93 applications on maintenance status.

3.4.4

Develop, manage, and support the Agency Web and Sharepoint sites and portals. These are new development efforts. Directorate Web and Sharepoint sites are the directorate Webmaster's responsibility. The contractor shall provide technical guidance and advice to the directorate Webmasters. The contractor shall develop and maintain the Web site. Web-development software of choice in the command includes MS FrontPage and Dreamweaver.

3.5 CONFIGURATION MANAGEMENT

3.5.1

Establish and maintain an effective configuration management program that incorporates a progressive configuration management maturity model in the management of the networks and its operations. The configuration management program shall define the configuration items, establish and document the configuration management processes, improve on the current configuration control and change management process, establish release baselines/documentation, establish a verification process, and other areas of Configuration Management Governance. Automated tools will be used for a positive return on investment (ROI). This configuration management program shall be planned, documented and established with direct coordination and phase approval of the government.

3.5.2

Be prepared to discuss the status of each LAN or any other topic associated with the LAN in accordance with this PWS. The contractor shall not make any changes, modifications, or upgrades to the LAN without the explicit approval of the COR.

3.5.3

Establish and maintain configuration control of all IT/IM systems as well as the LANs' hardware and software. Any changes to the configuration process shall be an automated process (diagrams), not a manual process and approved by COR. The contractor shall review, update, and maintain the configuration description documents and diagrams for all configurations.

3.5.4

Attend configuration control board meetings and brief the Government on status on a monthly basis. This briefing shall include updated diagrams of all networks. The contractor shall submit a Scientific and Technical Report.

3.5.5

Maintain and manage an integrated hardware and software asset inventory database.

3.5.6

Make effective use of available automated tools to execute the Configuration Management Program. Current tools in use at the Agency include Computer Associates' (CA) Unicenter Advanced Help Desk, Server Management System (SMS), SCALABLE, CISCO Works, DHCP, and AutoCAD Lite software packages to maintain and manage the asset inventory database; maintain information about the IT equipment such as asset number, Internet protocol (IP) address, host name, directorate, room number, telephone number, and building were the hardware or software is located; and use CiscoWorks LAN Management Solution (LMS) to track network switches' port density. The Government is planning the transition and expansion of the Computer Associates AHD product to incorporate CM/CC modules. This transition will required the implementation of another Computer Associates Unicenter-like application and cable infrastructure management software.

3.6 HELP DESK SERVICES

3.6.1

The contractor shall operate a level-one, consolidated customer help desk to serve as the single point of contact (POC) to answer IT/IM trouble calls for approximately 3,000+ end users. The Government operates a 24x7 call center that conducts preliminary assessment of a call and opens/dispatches work orders to other sections of the Agency. The contractor shall staff the help desk from 0600 to 1800hrs, Monday through Friday. This schedule is subject to change based on the Agency's requirement and may be required to cover longer hours, weekends or holidays at a future date. The contractor shall staff the help desk with qualified contractor employees trained in preliminary diagnostics and resolution of common user problems. The contractor shall provide preliminary screening of problems and requests and forward those issues that cannot be resolved by the help desk to the appropriate section, team, or contractor for action.

3.6.2

The contractor shall, upon receipt of a customer's trouble-call, perform the required assessment, utilizing remote access in doing so and if necessary, troubleshoot, isolate and resolve, or refer to the next level of help, the customer's problem. The help desk shall utilize a wide range of tools to address issues, including MS SMS to install or reinstall software if authorized and required. The workorder/incident management tool (HEAT) is used to record, dispatch, and manage work orders. The help desk shall monitor work order progress and shall ensure customers receive a work order number, status, and prompt resolution. The contractor shall document resolutions or action taken on each work order. Work orders should read easily to understand actions taken and current status. The help desk shall monitor work order progress in other sections to ensure the timely handling of customer work orders.

3.6.3

The help desk shall answer calls from General Officers (GO) received on the GO hotline immediately – not allowing them to go to voicemail. Work orders for General Officers and GO-equivalent members shall be handled as priority ONE (P-1), providing a path to resolution within the technically allowable timeframe. Resolution of these work orders may be postponed only when so coordinated with the flag officer.

3.6.4

Any P-1 work order that presents a technical or resource issue will be raised to and de-conflicted by the COR. Work orders of importance (but that may not be immediate) shall be handled as priority TWO. The default work order handling priority is a priority THREE. The help desk has a telephone call distribution system, but shall also receive work orders because of customer walk-ins. It is important that the customer support personnel be well trained in the art of customer interaction.

3.6.5 NETWORK MONITORING:

During operational hours, the help desk shall monitor the network management consoles for any outage. The help desk shall notify the appropriate section of any alarms or outages on the network. Network monitoring consoles shall be monitored at the Technical Control Facility (TCF) after the help desk closes. Network monitoring consoles are also present at the Current Operations section for daily monitoring by the system and network administrators.

3.6.6 REPORTABLE NETWORK OUTAGES:

The following equipment, services and facility outages shall be reported to the COR immediately:

Servers
Switches
Routers
Phone systems
Service outages to VIPs, which include all Officers and Senior Executive Service staff.

3.7 NETWORK MANAGEMENT SUPPORT

3.7.1

Install, configure, and manage all switches, routers, and other network infrastructure equipment. The contractor shall maintain routing tables, operating systems, security patches, and upgrades. The HQ building houses approximately 16 communications closets evenly distributed between SIPRNET and NIPRNET. Each communications closet supports a quadrant of the two-story building. The communications closet holds the patch panel and the CISCO 4500 switches that support the client network connections for that quadrant. The NIPRNET is a category (CAT) 5 network (CAT-5 Fast Ethernet to the workstation), and the SIPRNET is a fiber network (fiber Fast Ethernet to the workstation). One SIPRNET and one NIPRNET closets support satellite-site users. Each remote (satellite) site may also have a SIPRNET and NIPRNET closet that supports that segment. Approximately 113 CISCO switches and routers with the Internet Operating System (IOS) at or above version 12.4.19 comprise the entire HQ metropolitan area network.

3.7.2

Manage and control all wide area network IP ranges. The contractor shall act as the SIPRNET and NIPRNET Network Information Center's (NIC) technical POC for the Agency domains. The contractor shall coordinate with the region's network managers and the SIPRNET and NIPRNET NIC on all domain or IP issues. The HQ networks utilize fixed or static IP addressing, but may migrate to the Dynamic Host Control Protocol (DHCP) in the future.

3.7.3

Provide engineering and reengineering support for all new installs. The contractor shall provide reengineering support for current network infrastructure, ensuring lifecycle and network refresh is maintained.

3.7.4

Provide Domain Name Server (DNS) support for ASA- SOUTHCOM networks and provide secondary DNS support for the region's domains. The contractor shall provide guidance on standards to sub-domains on their DNS structure. This "external" DNS is a Red-hat LINUX Advance Server on a DELL Intel server. The "internal" DDNS resolves only for the internal network, and it runs the MS DDNS system. This second DNS is managed by the system administrators. (See PWS paragraph 3.1 Systems Administration.)

3.8 CABLE INFRASTRUCTURE SUPPORT

3.8.1

Provide vertical and horizontal, and fiber cable infrastructure support in accordance with the Electronic Industries Alliance (EIA) standards; repair or replace any defective fiber or copper cabling in the network; and report any outside-plant cabling outage to the telephone control officer (TCO).

3.8.2

Support all existing and new wiring and telecommunications closets. The contractor shall ensure wiring and patching is properly installed and labeled in accordance with EIA and Agency standards.

3.8.3

Provide support in the installation of new cabling infrastructure. The contractor shall install, remove, relocate, and maintain existing horizontal and vertical infrastructure, to include wall drop boxes, equipment racks, cable trays, rack-mounted uninterrupted power supplies (UPS), switches, routers, and servers. The contractor shall use Government-furnished equipment (GFE) to test and ensure that cabling meets EIA and Agency standards. CONUS construction is not permitted. Where cabling is being installed, the Government shall obtain the proper classification and send to the Contracting Officer to demonstrate that it is in fact equipment installation and not construction. No work shall be performed until approval by the Contracting Officer is received.

3.8.4

Record all inside-cabling changes on the existing CA Unicenter Advanced Help Desk automated work order system and on the AutoCAD Lite (LT) drawings. The contractor shall maintain engineering drawings in the most recent version of AutoCAD LT.

3.9 HARDWARE AND SOFTWARE SUPPORT

3.9.1

Provide integration, testing, evaluation, configuration control, and administration of desktop systems; perform integration and standardization of desktop hardware and software as required. New hardware and software testing is required to be performed by the contractor.

3.9.2

“Ghost” the standard NIPRNET and SIPRNET client baselines onto the workstations upon installation; load/deploy additional authorized software as required utilizing MS SMS and MS WSUS when deploying to a group of workstations, or with MS ‘remote access’ when deploying to an individual; perform on-site visits to load software as required. Approximately 250 different Government-off-the-shelf (GOTS) and commercial-off-the-shelf (COTS) software packages are loaded in different permutations in the 2,800 workstations (both SIPRNET and NIPRNET). Refer to Appendix 5 for an approximate list of these applications.

3.9.3

Test every new application for compatibility on the client and the network prior to installation; document every new application and its installation procedure on the network with technical instructions that will be followed by the help desk staff or by the technicians that perform the site visits; consult and coordinate with the vendor as required for troubleshooting, resolution, integration, and installation of the applications; and research, compare, and analyze software requirements and make recommendations on options and courses of actions.

3.9.4

Research, install, and Integrate new client-level hardware. Printers, multifunction printers, scanners, faxes, media drives, Blackberry/personal digital assistant (PDA) interfaces, etc., shall be researched, installed and integrated on the network.

3.9.5

Perform on-site (or remote-access) response to client or network problem isolation, troubleshooting, and service restoration.

3.9.6

Repair or replace hardware at the component level. If a problem cannot be resolved at this level, the contractor shall escalate the issue to the next level.

3.9.7

Propose software installs, removals, or upgrades to the Government for existing software upon their commercial release. The recommendations shall include the impact on the system and equipment as well as detailed cost of the change(s) and upgrade(s). The contractor shall submit any proposed changes to the COR for evaluation and approval prior to implementation. Upon receiving approval of the proposed upgrade(s), the contractor shall develop an implementation schedule.

3.10 VOICE NETWORK SUPPORT

3.10.1

Support secure and non-secure voice networks consisting of user telephone instruments, Secure Telephone Equipment (STE) instruments, and voice-over-IP (VoIP) network and instruments. The contractor shall provide on-site troubleshooting, problem isolation, and service restoration.

3.10.2

Coordinate maintenance and repair with service providers as necessary. The contractor shall coordinate through the Agency for any new telephone line requirement involving any cost or expense to the Government.

3.10.3

The contractor shall maintain, program, and operate the eOn Communications Millennium Digital Communications Platform telephone communications system. The Contractor shall provide staff certified on the the eOn system

3.11 ON-SITE AND ON-CALL SUPPORT

3.11.1

The contractor shall provide on-site system and network administration employees during normal duty hours (0600 to 1800, Monday through Friday). These hours may be covered on a shift schedule. Network problem identification and response times during normal duty hours shall be within 15 minutes. The contractor shall provide a two-hour response time after hours and on holidays. The on-call duty shall be required for the system administrators (servers), the VTC technicians, the IA section, and the network administrators (LAN/WAN, routers, and switches). Upon receiving notification, the contractor shall initiate actions to resolve major outages within two working hours of receipt of such notice, with the intent of restoring services as soon as possible. Any outage which affects senior staff is also defined as a major outage. The contractor shall provide a daily and a consolidated quarterly on-call

response/incident report that shall include the following data fields: Date, Technician Called, Time of Initial Call, Time of Technician Arrival, Brief Problem Description, and Time of Resolution.

3.11.2

The contractor shall work with Government and other contractor employees in troubleshooting problems that span the integrated IT/IM systems and networks, including nodal IT/IM systems supported by other contractors.

3.12 LICENSES AND WARRANTIES

The Government may require the contractor to procure COTS software and equipment during emergencies. Examples are: MS Software Suite, AUTOCAD, ADOBE-Suite, Photoshop, and Puredge. It is the intent that the Government will require the contractor to procure any COTS or hardware, licenses, warranties, equipment, and those COTS acquisitions will managed by the contractor (i.e., hardware, licenses, warranties, or equipment) and that any the COTS software and equipment be turned over to the Government at the termination of the contract.

Any commercial warranties that apply to incidental items purchased must be submitted to the Government for review.

3.13 WORK SITE

The contractor shall maintain work site and storage areas in accordance with local regulations and laws.

3.14 INSOURCING PLAN

In-sourcing is the conversion of currently contracted service to DoD civilian or military performance, or a combination of thereof. If a contracted position is in-sourced, the contractor shall not fill that position unless approved by the GTL.

3.15 QUALITY CONTROL (QC)

The contractor shall develop and implement a specific, simplified, and easily implemented Quality Control Plan (QCP) that identifies potential and actual problem areas in satisfying the requirements of this task order as specified and results in corrective action throughout the life of the Task Order. The plan shall identify the methods by which the contractor ensures the terms of this Task Order are met the contractor shall maintain support documentation for all actions taken over the life of the Task Order (e.g., work requests and inspection correction reports). These files shall be made available to the Government when requested by the KO or COR. Upon completion of the Task Order, the contractor shall turn all files over to the COR. In accordance with Contracts Data Requirement List (CDRL) B006, Quality Control Plan.

3.16 QUALITY ASSURANCE

The Government will evaluate the contractor's performance under this contract in accordance with the Quality Assurance Surveillance Plan (QASP). This plan is primarily focused on what the Government must do to ensure that the contractor has performed in accordance with the performance standards. It defines how the performance standards will be applied, the frequency of surveillance, and the minimum acceptable defect rate(s).

The performance requirements summary is at Appendix 1.

3.17 HOURS OF OPERATION

The contractor shall be responsible for conducting operations between the hours of 6am to 6pm Monday thru Friday, core hours being 7am to 4pm Monday thru Friday except Federal holidays or when the Government facility is closed due to local or national emergencies, administrative closings, or similar Government directed facility closings. The Technical Control Facility requires 24 hours a day and 7 days week coverage. The Contractor shall also provide on-

call coverage by the system administrators, network administrators, VTC, and network security administrators. The Command will require system administrator, helpdesk, VTC, and other services during real-world contingencies as well as during exercises. The contractor shall be flexible to support these during off-hours, weekends, and holidays.

Key personnel shall be required to remain on-site during a hurricane or destructive weather situation to maintain or oversee networks along with identified government personnel. All contractor employees shall be required to comply with and abide by the Government's alert roster reporting procedures.

The Contractor shall maintain an adequate work force for the uninterrupted performance of all tasks defined within this performance work statement when the Government facility is not closed for the above reasons. When hiring personnel, the Contractor shall keep in mind that the stability and continuity of the work force are essential. Contractor shall identify a retention plan to retain subject-matter-experts on hand and submit a Scientific and Technical Report in accordance with Contracts Data Requirement List (CDRL) B001 and DI-MISC-80711A.

3.18 SPECIAL REQUIREMENTS

3.18.1 INVOICE REPORT

The contractor shall submit, on a monthly basis, an Invoice Report in accordance with the Government supplied format and Contracts Data Requirement List (CDRL) B007 and DI-MGMT-80004A. See attached Appendix-2 for the format.

3.18.2 TRAINING OF CONTRACTOR EMPLOYEES

The contractor shall provide employees with the required core skills to perform their job duties. Otherwise, training to build or maintain expertise of contractor employees assigned to this Task Order shall be provided by the contractor at its own expense except when the Government has given prior approval for training to meet special requirements that are peculiar to a particular task. In addition to the core competencies related to their jobs, the contractor shall ensure that the employees are trained on customer support protocols and customer relations. The contractor shall ensure that their employees are trained on the protocols associated with the support of all ranks of the military, civilian, contractor, and interagency members of a Joint Command. Limited training of contractor employees may be authorized when the Government changes IT/IM software or hardware during the performance of an ongoing task and it is determined to be in the best interest of the Government. Contractor employees shall attend seminars, symposiums, or user group conferences only if the Government certifies that attendance is mandatory for the performance of the task requirements and the COR approves such training in advance. Reimbursement for training shall not be authorized for replacement contractor employees; for the purpose of keeping contractor employees abreast of advances in the state of the art; nor for training contractor employees on equipment, computer languages, or computer operating systems that are available on the commercial market. The contractor shall have full responsibility for keeping contractor employees trained and abreast of advances in the standard commercial and network technologies implemented in the Agency.

3.18.3 CERTIFICATION OF CONTRACTOR EMPLOYEES

The contractor shall ensure the certification compliance IAW DoD 8570.01-M Information Assurance Workforce Improvement Program. The contractor personnel shall agree as a "condition of employment" to obtain the appropriate baseline certification upon contract award. The contractor shall ensure that all TIER I/TIER II support personnel obtain and maintain certification corresponding to Information Assurance Technical Level I (IAT I). Contractor employees performing functions as Application Support are required to obtain and maintain certification corresponding to Information Assurance Technical Level II (IAT II). Contractor employees performing functions as Systems administrators/Enterprise Management are required to obtain and maintain certification corresponding to Information Assurance Technical Level II (IAT II). Contractor employees performing functions as Network Technicians are required to obtain and maintain certification corresponding to Information Assurance Technical Level III (IAT III). Contractor employees performing functions as Engineers are required to obtain and maintain certification corresponding to Information Assurance Technical Level III (IAT III). Contractor employees performing functions as Network Security Technicians are required to obtain and maintain certification corresponding to Information Assurance Technical Level III (IAT III). The contractor shall ensure all employees

meet the minimum requirements within six months of the task order award. Further, the contractor shall ensure all new hires meet the minimum requirements for their respective positions upon initiation of their duties. Contractor Technical Level I, II and III personnel must also obtain the appropriate computing environment certification/s required by their employing organization. The contractor shall be responsible for yearly maintenance fees to keep these certifications. This includes but is not limited to 120 Continuing Professional Education credits (CPEs) every three years.

3.18.4 ACQUISITION REQUIREMENTS

The contractor shall be required to obtain replacement hardware and software required to perform this order as needed during catastrophic recovery and support. A catatastrophy for the purposes of this order is if a critical IT network component fails and cannot be timely replaced by other contracting means.. All materiel acquisition support shall be approved in advance in writing by the COR. Equipment purchased by the contractor under this Task Order shall require Information Assurance Vulnerability Assessment (IAVA) scanning and patching prior to allowing connectivity to the Government production network. Items obtained shall become the property of the Government and shall be added to the appropriate property book records. The contractor is required to establish a Government-furnished property (GFP) hand-receipt using the Defense PBUSE System with the supporting Property Book Officer (PBO). Only material in support of the service of this task order shall be acquired.

The Government pre-establishes the ceiling for this support at $50,000.00 per period.

3.18.5 TASKS

The contractor shall not perform any tasks under this task order that constitute work of policy, decision making, or of a managerial nature that is the direct responsibility of the Government.

3.18.6 KEY PERSONNEL

Key Personnel Qualification Matrix of the Alliant contract contains the contract labor category descriptions. The contract labor category descriptions provide the minimum qualifications for the labor categories proposed in Section B of this task order request.

Designate the minimum personnel that will be considered key personnnel and assigned to this task order. The contractor shall propose appropriate labor categories for this (these) position(s). Key personnel must be assigned for the duration of the task order. The Government encourages and will evaluate additional key personnel as proposed by the contractor.

- One (1) Contractor Program Manager
- One (1) Contract Administrator

4.0 TRAVEL

The contractor shall be required to travel CONUS (any state in USA) and OCONUS (any country in Central, South America, and the Caribbean to accomplish the tasks contained in this Task Order.

Costs for transportation may be based upon mileage rates, actual costs incurred, or a combination thereof, provided the method used results in a reasonable charge. Travel costs will be considered reasonable and allowable only to the extent that they do not exceed on a daily basis, the maximum per diem rates in effect at the time of the travel. The Joint Travel Regulations (JTR), while not wholly applicable to contractors shall provide the basis for the determination as to reasonable and allowable. Maximum use is to be made of the lowest available customary standard coach or equivalent airfare accommodations available during normal business hours. All necessary travel meeting the above criteria shall be approved in advance by the COR. Exceptions to these guidelines shall be approved in advance by the Contracting Officer.

5.0 GOVERNMENT USE OF DATA

Reference DFAR clause (252.227-7014) Rights in Non-commercial Computer software and noncommercial computer software documentation. The Government requires unlimited rights in any material first produced in the performance of this task order, in accordance with the FAR clause at 52.217-14. In addition, for any material first produced in the performance of this task order, the materials may be shared with other agencies or contractors during the period of performance of this task order, or after its termination. For any subcontractors or teaming partners, the Contractor shall ensure at proposal submission that the subcontractors and /or teaming partners are willing to provide the data rights required under this task order.

The Government intends to use this information on future Government requirements.

6.0 ORGANIZATIONAL CONFLICT OF INTEREST

If the contractor is currently providing support or anticipates providing support to the U.S. Army that creates or represents an actual or potential organizational conflict of interest (OCI), the contractor shall immediately disclose this actual or potential OCI in accordance with FAR Part 9.5. The contractor is also required to complete and sign an Organizational Conflict of Interest Statement in which the contractor (and any subcontractors, consultants or teaming partners) agree to disclose information concerning the actual or potential conflict with any proposal for any solicitation relating to any work in the TO. All actual or potential OCI situations shall be handled in accordance with FAR Subpart 9.5.

7.0 NON DISCLOSURE REQUIREMENTS

All contractor personnel (to include subcontractors, teaming partners, and consultants) who will be personally and substantially involved in the performance of the TO issued which requires the contractor to act on behalf of, or provide advice with respect to any phase of an agency procurement, as defined in FAR 3.104-4, shall execute and submit an "Employee/Contractor Non-Disclosure Agreement" Form. This is required prior to the commencement of any work on such TO and whenever replacement personnel are proposed under an ongoing TO. Any information obtained or provided in the performance of this TO is only to be used in the performance of the TO.

8.0 ACCESS TO GOVERNMENT SYSTEMS

In accordance with DoD Directive Number 7045.14, dated 21 November 2003, contractors are not allowed access to any DOD system including Program-Planning Budgeting System without explicit authorization of a relevant Government official, and that is based on a need-to-know basis only. Individuals granted access must have the appropriate clearance for access to a particular system.

9.0 TASK ORDER CLOSEOUT

The contractor shall submit a final invoice within forty-five (45) calendar days after the end of The Performance Period. After the final invoice has been paid the contractor shall furnish a completed and signed Release of Claims to the Contracting Officer. This release of claims is due within fifteen (15) calendar days of final payment.

10.0 PAST PERFORMANCE INFORMATION

In accordance with FAR 42.15 Contractor Performance Information, past performance evaluations shall be prepared for each task order that exceeds the simplified acquisition threshold placed against a Government-wide Acquisition Contract. For severable task orders, interim evaluations will be required prior to exercising any option periods. For non-severable task orders, evaluations must be collected, coordinated and reported upon completion of the task order.

The Government will provide and record Past Performance Information for acquisitions over $100,000 utilizing the Contractor Performance Assessment Reporting System (CPARS). The CPARS allows contractors to view and comment on the Government's evaluation of the contractor's performance before it is finalized. Once the contractor's past performance evaluation is finalized in CPARS it will be transmitted into the Past Performance Information Retrieval System (PPIRS).

Contractors are required to register in CPARS, so contractors may review and comment on past performance reports submitted.

Contractors must register at the following websites:

CPARS: http://www.cpars.csd.disa.mil/

PPIRS: http://www.ppirs.gov/

11.0 CONTRACTOR'S PURCHASING SYSTEMS

The objective of a contractor purchasing system assessment is to evaluate the efficiency and effectiveness with which the contractor spends Government funds and complies with Government policy with subcontracting.

Prior to the award of a task order the Contracting Officer shall verify the validity of the contractor's purchasing system. Thereafter, the contractor is required to certify to the Contracting Officer no later than 30 calendar days prior to the exercise of any options the validity of their purchasing system. Additionally, if reviews are conducted of the purchasing system after the exercise of the option, the contractor shall provide the results of the review to the Contracting Officer within 2 weeks from the date the results are known to the contractor.

12.0 PRIVACY ACT

Work on this project may require that personnel have access to Privacy Information. Personnel Shall adhere to the Privacy act, Title 5 of the U.S. Code, Section 552a and applicable agency rules and regulations.

13.0 NOTICE OF THE FEDERAL ACCESSIBILITY LAW AFFECTING ALL ELECTRONIC AND INFORMATION TECHNOLOGY PROCUREMENTS (SECTION 508)

On August 7, 1998, Section 508 of the Rehabilitation Act of 1973 was amended to require that when Federal departments or agencies develop, procure, maintain, or use Electronic and Information Technology, that they shall ensure it allows Federal employees with disabilities to have access to and use of information and data that is comparable to the access to and use of information and data by other Federal employees. Section 508 required the Architectural and Transportation Barriers Compliance Board (Access Board) to publish standards setting forth a definition of electronic and information technology and the technical and functional criteria for such technology to comply with Section 508. These standards have been developed are published with an effective date of December 21, 2000. Federal departments and agencies shall develop all Electronic and Information Technology requirements to comply with the standards found in 36 CFR 1194.

14.0 SECTION 508 – ELECTRONIC AND INFORMATION TECHNOLOGY (EIT) STANDARDS

The Section 508 standards established by the Architectural and Transportation Barriers Compliance Board (Access Board) are incorporated into, and made part of all VA orders, solicitations and purchase orders developed to procure Electronic and Information Technology (EIT). These standards are found in their entirety at: http//www.section508.gov and http://www.access-board.gov/sec508/standards.htm. A printed copy of the standards will be supplied upon request. The Contractor shall comply with the technical standards as marked:

_x_ § 1194.21 Software applications and operating systems

_x_ § 1194.22 Web-based intranet and internet information and applications

_x_ § 1194.23 Telecommunications products

_x_ § 1194.24 Video and multimedia products

_x_ § 1194.25 Self contained, closed products

_x_ § 1194.26 Desktop and portable computers

_x_ § 1194.31 Functional Performance Criteria

_x_ § 1194.41 Information, Documentation, and Support

The standards do not require the installation of specific accessibility-related software or the attachment of an assistive technology device, but merely require that the EIT be compatible with such software and devices so that it can be made accessible if so required by the agency in the future.

15.0 POINTS OF CONTACT

The following Points of Contact should be utilized for this order:
Contracting Officer: xxxx

Contracting Officer's Representative (COR): xxx

16.0 FEDERAL ACQUISITION REGULATION (48 CFR CHAPTER 1) SOLICITATION CLAUSES (HTTP://WWW.ARNET.GOV/FAR/)

NOTE: Paragraphs I.1 through I.14 of the contractor's awarded Alliant GWAC contract are applicable to this Task Order and are hereby incorporated by reference. In addition, the following applies.

CLAUSE NO	CLAUSE TITLE	DATE
52.217-9	OPTION TO EXTEND THE TERM OF THE CONTRACT	(MAR 2000)
52.217-8	OPTION TO EXTEND SERVICES	(NOV1999)
52.227-14	RIGHTS IN DATA – GENERAL ALTERNATE V	(JUN 1987)
52.245.19	GOVERNMENT FURNISHED PROPERTY "AS IS"	(APR 1984)

DEFENSE FEDERAL ACQUISITION REGULATION SUPPLEMENTS (DFARS) CLAUSES INCORPORATED BY REFERENCE

CLAUSE NO	CLAUSE TITLE	DATE
252.204-7004	Required Central Contractor Registration	(Nov 2001)
252.227-7013	Rights in Technical Data - Noncommercial Items	(Nov 1995)
252.227-7014	Rights in Noncommercial Computer Software and Noncommercial Computer Software Documentation	(Jun 1995)
252.227-7016	Rights in Bid or Proposal Information	(Jun 1995)
252.227-7019	Validation of Asserted Restrictions - Computer Software	(Jun 1995)
252.227-7028	Technical Data or Computer Software Previously Delivered to the Government	(Jun 1995)
252.246-7001	Warranty of Data	(Mar 2003)

17.0 INVOICING

The Contractor shall submit Requests for Payments in accordance with the format contained at a minimum include the following information to have the invoice considered proper for payment.

(a) Contract number;

(b) Paying Number: (ACT/DAC NO.);

(c) Applicable CLIN or Sub-CLIN in which the costs were incurred, quantity, unit price and extended price;

(d) If applicable, incurred cost of all approved travel to include name of Government approving official and date approved;

(e) List of all applicable materials and/or services provided under this order to include the part number, nomenclature, quantity, and the unit and extended price;

The Contractor shall include the following statement on all invoices submitted for payment: "The costs and pricing contained within this invoice do not exceed the allowable costs of the applicable Government contract."

The Contractor shall ensure that all requests for payments are validated, signed and dated by the Contracting Officer's Representative of this task order before payment. The invoice shall include the following statement. "I, *printed name of Government POC*, have verified that in a satisfactory manner the items identified have been received or the services have been rendered and I take no exceptions to this invoice."

18.0 APPENDICES

1. Quality Assurance Survaillance Plan (QASP)
2. Contracts Data Requirement List (CDRL) A001-B007

Appendix 1 – Performance Requirements Summary

Performance standards define desired services. The Government performs surveillance to determine if the contractor exceeds, meets or does not meet these standards.

The following matrix includes performance standards. The Government shall use these standards to determine contractor performance and shall compare contractor performance to the Acceptable Quality Level (AQL).

Performance Based Task	Indicator	Standard	Acceptable Quality Level	Method of Surveillance	Incentive
Systems Administration	Provide continuous network on-call support 24/7.	Maintain LAN systems services not less than 98% availability per year.	Not more than 1 failure per yearly period of performance.	Observation.	Exercise of Option Year and past performance evaluation.

Information Assurance	Provide continuous network security systems outages, spillages, and firewalls support 24x7.	Maintain system security administration not less than 98% availability per year.	Not more than 1 failure per yearly period of performance.	Observation.	Exercise of Option Year and past performance evaluation.
Database, Help Desk, Network Management Support	Provide continuous database, help desk and network operations 24X7.	Maintain database, help desk and network administration not less than 98% availability per year.	Not more than 1 failure per yearly period of performance.	Observation.	Exercise of Option Year and past performance evaluation.
On-Call/Site Support	Provide continuous on-call/site system operations 24/7.	Maintain system on-call/site network support not less than 98% availability per year.	Not more than 1 failure per yearly period of performance.	Observation.	Exercise of Option Year and past performance evaluation.
Technical Control Facility	Provide electronic maintenance support 24/7.	Maintain electronic maintenance support not less 98% availability per year.	Not more than 1 failure per yearly period of performance.	Observation.	Exercise of Option Year and past performance evaluation.