Section C – Descriptions/specifications/statement of work

**R2-3G PERFORMANCE WORK STATEMENT (PWS)**

**24October 2012**

**3G-0583**

**8A C4i Deployable IT Support**

**1.0 SCOPE Description of Services**

Contractor shall provide all personnel, equipment, supplies, transportation, tools, materials, supervision, and

other items and non-personal services necessary to perform command, control, communications, and computer information (C4i) systems support as defined in this performance-based work statement (PWS) except for

those items specified as government furnished property. Contractor shall perform to the standards identified in this contract.

**Vision**

Enable Eighth Army (8A) Command and Control through unclassified and classified network-centric warfare in support of the Korean Theater of Operations (KTO) by designing and maintaining a distributed, web-enabled, and mission-oriented deployable capability through a ubiquitous tactical network environment filled with reliable, available, and secure information that is of value to the Warfighter.

**Mission**

Establish, provide, and implement/maintain to standards and operational requirements C4i capability to support combined US and Republic of Korea (ROK) operations in Korea and when deployed in the Pacific or as part of ARFORGEN. Provide the 8A Commander’s staff, and selected organizations with C4i services that enable them, through establishment of efficient, effective, and collaborative C2 capabilities, to effectively command and control deployed, combat-ready troops in the Pacific or elsewhere through net-centric high-speed connectivity among sites supporting ROK, US, and/or Coalition forces.

**Background**

All work is related to C4i. Information Technology has transformed traditional battlefield functions. Emerging applications of IT will result in full realization of net-centric warfare. This net-centric environment has caused the

Global Information Grid (GIG) to evolve into a complex web, which makes it challenging for 8A to maintain

cognizance over its C4i networks. The number and complexity of its C4i systems and networks is rapidly outgrowing our ability to manage them. As a result, a robust net-centric infrastructure is fundamental to accomplishing the 8A mission.

**1.1 GENERAL**

Contractor employees performing services under this contract shall be controlled, directed and supervised at all times by management personnel of the contractor. The contractor's management shall ensure that employees properly comply with the performance standards outlined in this Performance Work Statement and as required by the contracting officer or the contracting officer's representative (COR). Contractor employees shall perform

independent of and without the supervision of any Government official. Actions of contractor employees may not be interpreted or implemented in any manner that results in any contractor employee creating or modifying Federal policy, obligating the appropriated funds of the U.S. Government, overseeing the work of Federal employees, providing direct personal services to any Federal employee or otherwise violating the prohibitions set forth in Parts

7.5 and 37.1 of the Federal Acquisition Regulation (FAR). The Government shall control access to the facility and shall perform the inspection and acceptance of completed work and tasks.

**1.2 APPLICABILITY**

This Task PWS applies to paragraphs 4.1, 4.8, and 4.11 of the R2-3G PWS (Section J, Attachment 01).

**1.3 TASK ORDER PERIOD OF PERFORMANCE / PLACE OF PERFORMANCE**

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

1.3.3 Performance will take place, but is not limited to USAG Yongsan, South Korea; USAG Daegu, South Korea; USAG Red Cloud, South Korea; and USAG Humphreys, South Korea. Contractor shall also provide Government with support, upon Government notification, at any US or ROK Government site on-peninsula.

**1.4 CONTRACT MANAGEMENT**

All requirements of paragraph 3.3 and 3.12.1 of the R2-3G PWS apply to this effort. This task order shall be addressed in the Contractor’s Progress, Status and Management Report required by DI-MGMT-80227 and CDRL D001.

**1.4.1 Army Contractor Manpower Reporting System**

As stated in paragraph 3.5 of the PWS, Army Contractor Manpower Reporting System requirements apply to this effort and all manpower requirements shall be input into System as required.

To fulfill this Army reporting requirement, the following COR’s information is provided:

**The Unit Identification Code (UIC) for the Contracting Officer Representative is: WJS7AA.**

**The Federal Service Code (FSC) for the Contracting Officer Representative is: D307 and D316 . The Command Code for the Contracting Officer Representative is: 820.**

**Fiscal Funding Station Code: S92127.**

**1.5 GOVERNMENT FURNISHED EQUIPMENT / MATERIALS / FACILITIES**

The Government will provide physical work space and will furnish: desk, phone, computer equipment (to include all necessary hardware & software), an electronic mail (e-mail) account, use of the Government telephone, facsimile machine, copier usage, as required by this position.

**1.5.1** GFE includes a computer system, workstation, and workplace supplies.

**1.6 INSPECTION and ACCEPTANCE**

Inspection and acceptance shall be at **Yongsan Army Garrison, Korea. Ship to address is: PSC 303, Box 74, APO AP 96204.**

**Requiring Activity’s DODAAC: WQ0QT2 . When the effort is proposed using CPFF or**

**T&M.**

**Accepting Activity DODACC:**

**WQ0QT2**

**. When the effort is proposed using CPFF.**

**1.7 SECURITY**

**1.7 Security Management**

Contractor shall provide C4I Customers with expert security management. Contractor shall strictly adhere to all applicable security regulations, requirements, and procedures while fulfilling its information, operations, personnel, and physical security responsibilities, including security administration, handling and storage of classified information, and, if necessary, security incident reporting. Contractor shall document management support procedures in Security Management SOP.

1.7.1 Security Administration

Contractor shall identify security responsibilities on Government-provided DD Form 254 “Contract Security

Classification Specification.”

1.7.2 Handling and Storage of Classified Information

Contractor shall strictly adhere to all applicable security regulations, requirements, and procedures concerning handling and storage of classified information.

1.7.3 Personnel Security

Contractor shall strictly adhere to all applicable personnel security regulations, requirements, and procedures.

1.7.3.1 Joint Personnel Adjudication System (JPAS)

Government will establish ADP/IT positions in JPAS for each Contractor position.

1.7.3.2 Security Clearances

Contractor shall obtain appropriate security clearance for each employee to ensure s/he has access to perform required services.

1.7.3.2.1 FINAL US SECRET

Contractor shall ensure that only its personnel who possess FINAL US SECRET security clearances have access to

US SECRET C2 systems and environments (e.g., server rooms and communications closets).

1.7.3.2.2 TOP SECRET

Contractor shall ensure that at least one of its Security Management personnel possesses a US SECRET security clearance (Amendment 0001). If the Government determines that the Security Management contractor employee

who is supposed to possess a US SECRET security clearance does not possess a US SECRET security clearance, the Government reserves the right to require the Contractor to provide a new Security Management contractor employee who possesses a US SECRET security clearance, at no additional cost to the Government. Additionally, the

Government reserves the right, at its sole discretion, to recoup the costs of the salary of the US SECRET security

clearance employee from the Contractor during the time-period that there was no Security Management contractor employee with a US SECRET security clearance available for the Government’s use.

1.7.3.2.3 SECRET, US Citizen

Contractor shall ensure that only its personnel who possess “SECRET, US Citizen” security clearances have access to SECRET C2 systems and environments.

1.7.3.3 Badges

All Contractor personnel shall wear Contractor identification badges and a government-supplied badge or common access card (CAC) at all times while on government property.

1.7.3.4 Security Violation Reporting

Contractor shall promote a high level of security awareness among its personnel, formally train its personnel, and take appropriate precautions to prevent security violations. However, if a Contractor does commit or observe a possible security violation, s/he shall report the incident immediately to 8A G2.

1.7.3.5 Substitution or Replacement.

1.7.3.5.1 Substitution/Replacement Qualifications

Contractor shall only substitute or replace an employee with one who has security clearance and security investigation qualifications equal to or higher than those of the person being replaced.

1.7.3.5.2 Substitution/Replacement Notification

When Contractor decides to substitute or replace an employee, Contractor shall notify Government and Customer at least ten business days prior (except in emergencies). Notification shall include:

1.7.3.5.2.1 Substitution/Replacement Explanation

Contractor shall explain circumstances necessitating action.

1.7.3.5.2.2 Substitution/Replacement Position Requirements

Contractor shall identify security clearance, security investigation level, and technical qualification requirements of the position.

1.7.3.5.2.3 Substitution/Replacement Qualifications

Contractor shall identify security clearance, security investigation level, and technical qualifications of proposed substitute or replacement.

1.7.3.6 Transfer or Termination

When Contractor transfers or terminates an employee, Contractor shall immediately:

1.7.3.6.1 Access Revocation

Revoke employee’s access to all applicable contract-provided systems and services.

1.7.3.6.2 Badge Turn-in

Collect employee’s applicable identification badges and contract-related documents, and turn-in to Government.

1.7.3.7 Employee Removal

Government may prohibit a Contractor employee access to work site if Government determines that the employee is a security risk.

1.7.3.8 Personnel Security Administration

DD Form 254 “DoD Contract Security Classification Specification.” Contractor shall assist Government in filling out DD Form 254 "Department of Defense Contract Security Classification Specification" and verify that Contractor's information is correct.

1.7.4 Physical Security

Contractor shall perform Physical Security duties at all 8A C4I sites IAW all applicable physical security regulations, requirements, and procedures.

1.7.5 Security Incident Reports.

1.7.5.1 Initial Security Incident Report

Contractor shall provide Customer with an Initial Incident Report NLT one hour after incident notification.

1.7.5.2 Final Security Incident Report

Contractor shall provide Customer with a Final Incident report NLT two hours after incident resolution.

**1.8 Key Personnel**

The Contractor shall provide a work force possessing the skills, knowledge, clearances and training to satisfactorily perform functional and technical support to meet the telecommunications required support. The following are considered key personnel:

**1.8.1 Telecommunication Specialists (3) R2-3G Labor Category #96**

The Telecommunication Specialists shall meet the minimum qualifications of the R2-3G base contract Labor Category #96. In addition to those requirements, the Telecommunication Specialist shall have a minimum of four (4) years experience within the last six (6) years of Tier 2 Technical Support for the ongoing operations and support of the Command Center Suite systems. Tier II includes maintaining and improving the current voice, data and video technical support for Command Center systems supported by the customer, and provides cost effective, consolidated maintenance services. The Telecommunication Specialists shall demonstrate that they have experience in performing tests and evaluations of new or upgraded equipment and services to include system cutover, capacity and performance testing, maintenance and systems acceptance. The individual shall demonstrate that they have experience in ensuring all configuration management products are updated to reflect new installations or changes in configuration. The Telecommunication Specialists shall be Information Assurance Technical (IAT) level II-certified.

**1.8.2 Telecommunication Specialists, Senior (2) R2-3G Labor Category #97**

The Telecommunication Specialists, Senior shall meet the minimum qualifications of the R2-3G base contract Labor Category #97. In addition to those requirements, the Telecommunication Specialist shall have a minimum of six (6) years experience within the last eight (8) years of Tier III Technical Support for the ongoing operations and support of the Command Center Suite systems. Tier III includes evaluating communication hardware and software, troubleshooting LAN/MAN/WAN and network related problems, providing technical expertise for performance and configuration of networks, scheduling conversions and cutovers, overseeing network control center and supervising maintenance of systems. The individual shall demonstrate that they have experience ensuring all configuration

management products are updated to reflect new installations or changes in configuration. The Telecommunication

Specialist, Senior shall be Information Assurance Technical (IAT) level III-certified.

**1.8.3 Senior INFOSEC Engineer (1) R2-3G Labor Category #149**

The Senior INFOSEC Engineer shall meet the minimum qualifications of the R2-3G base contract Labor Category #149. In addition to those requirements, the Senior INFOSEC Engineer shall have a minimum of five (5) years experience within the last seven (7) years of system administration and Computer Network Defense (CND). Personnel shall also have no less than three (3) years of which two (2) years has occurred within the last two (2) years experience with Host Based Security Systems (HBSS).

Personnel shall have a COMPTia Security Plus, a government approved computing environment, and Advanced HBSS 4.0 certificates. They shall also be Information Assurance Technical (IAT) III and IA Workforce System Architect and Engineer (IASAE) Level III-certified.

**1.8.4 Computer Systems Analyst, Intermediate (2) R2-3G Labor Category #90**

The Computer Systems Analyst, Intermediate shall meet the minimum qualifications of the R2-3G base contract Labor Category #90. In addition to those requirements, the Computer System Analyst, Intermediate shall be Information Assurance Technical (IAT) level II-certified.

**1.8.5 Program Analyst, Journeyman (1) R2-3G Labor Category #41**

The Program Analyst, Journeyman shall meet the minimum qualifications of the R2-3G base contract Labor Category #41. In addition to those requirements, the Program Analyst, Journeyman shall be Information Assurance Technical (IAT) level I-certified.

**1.8.6 Web Application Developer (1) R2-3G Labor Category #95**

The Web Application Developer shall meet the minimum qualifications of the R2-3G base contract Labor Category

#95. In addition to those requirements, the Web Application Developer shall be Information Assurance Technical

(IAT) level II-certified.

**3.0 REQUIREMENTS**

The contractor, as an independent contractor and not as an agent of the

Government, shall provide the necessary resources (except those furnished by

the Government) to accomplish tasks of the type set forth below. Contractor’s core areas of responsibility are C4i engineering and integration; technical support; information assurance, and program analysis support. These responsibilities cover networks, systems and services, tool sets, and IT devices used throughout the Korean Theater. Contractor shall provide effort and resources under this contract to support 8A C4i Customers throughout the Korean Theater of Operations (KTO).

**3.1 Networks and Systems Supported**

Contractor shall support Networks and Systems which serve US and/or Coalition forces. These networks provide gateways to existing military network enclaves, thus allowing shared access to C4i systems and services across the tactical enterprise.

3.1.1 US-Secret Communications Networks

Contractor shall support US-Secret Communications Networks.

3.1.1.1 US-Secret Command and Control (C2) Systems

Contractor shall support US-Secret C2 systems on US-Secret Tactical Communications Networks.

3.1.1.2 US-Secret Office Automation (OA) Systems

Contractor shall support US-Secret OA systems, including collaboration tools, on US-Secret Tactical

Communications Networks.

3.1.2 US-Unclassified Communications Tactical Networks

Contractor shall support US-Unclassified Tactical Communications Networks.

3.1.2.1 US-Unclassified Command and Control (C2) Systems

Contractor shall support US-Unclassified C2 systems on US-Unclassified Tactical Communications Networks.

3.1.2.2 US-Unclassified Office Automation (OA) Systems

Contractor shall support US-Unclassified OA systems on US-Unclassified Tactical Communications Networks.

3.1.3 US-Unclassified but Sensitive Communications Networks / Office Automation (OA) Systems

Contractor shall support US-Unclassified but Sensitive Tactical Communications Networks and Office Automation

(OA) Systems, including collaboration tools, on those networks.

**3.2 Scope of Responsibilities.**

3.2.1 Overall Government Responsibilities

Government will, throughout the life of this contract:

3.2.1.1 Operations Governance

Government will provide governance, oversight, and monitoring of Contractor’s operations.

3.2.1.2 Network Ownership

Government will retain both ownership and operation of applicable C4I tactical networks.

3.2.1.3 Approval Authority

Government will retain authority to approve changes.

3.2.2 Overall Contractor Responsibilities

Contractor shall, during the execution of all tasks identified within this PWS:

3.2.2.1 Comprehensive C4I Solutions

Contractor shall provide Government with comprehensive C4I solutions when issues arise to include network availability, integration, interoperability, and QoS. Contractor shall comply with all applicable Government directives, including regulations, supplements, instructions, and standards; and IT industry standards. Contractor shall comply with the latest published version of each Government directive and IT Industry standard as of the date the Contractor executes each task.

3.2.2.2 Employee Supervision

Contractor shall provide all employees with conscientious supervision and proactive direction.

3.2.2.3 Non-Disclosure Statements

Contractor employees shall sign non-disclosure statements prior to the beginning of any work the Government deems sensitive enough to warrant such action.

**3.3 Contractor Personnel Qualifications**

3.3.1 Security Clearance and Investigation Qualifications

Contractor shall ensure that all employees possess security clearance and security investigation necessary to perform required services in required location(s) at contract transition period start date and keep those qualifications up-to- date IAW official Government guidelines.

3.3.2 Contractor Training Requirements

Contractor shall ensure that its employees are fully trained to be able to fulfill this contract’s requirements.

3.3.3.1 Contractor Training Registration

Contractor shall ensure that all applicable Contractor personnel register in the official Government training certification system, which currently is the Army Training Certification and Tracking System (ATCTS), NLT three working days after obtaining common access card (CAC) pertaining to this contract. Contract’s Government Responsible Officer (RO) will assist Contractor in obtaining CACs for its personnel.

3.3.3.2 Training Support to Contractor

Government may provide Contractor with training at government cost for unique systems employed on the C4i networks supported by this contract to enable Contractor personnel to fulfill their requirements to this contract as skillfully and professionally as possible. Government will not reimburse Contractor for the cost of any employee training or labor involved with any commercially available, industry standardized training, or any course not unique and specific to this contract's requirements. No Government-funded Contractor training shall be conducted without the Government's advance, written approval.

3.3.3.3 Government Courses

Contractor may, with Government approval, permit its employees to attend Government-sponsored courses, seminars, or conferences, which are intended for Government audiences on a space-available basis if the courses support contract requirements.

3.3.3.4 Contractor Technical Qualifications

Contractor shall ensure that all employees possess required credentials; meet required technical, information assurance (IA), computing environment, and training certification and license requirements; and pass minimum experience qualification standards commensurate with their positions and responsibilities at contract transition

period start date and keep those qualifications up‐to‐date IAW DoD Instruction 8570.01‐M. The contractor shall ensure that personnel accessing information systems have the proper and current information assurance certification to perform information assurance functions in accordance with DFARS Clause 252.239-7001, which will be included in the awarded task order.

3.4 Exercise Support.

Contractor shall provide Government with exercise support. Government will conduct at least two major exercises lasting 21 days each and two minor exercises lasting 10 days each annually. Government will notify Contractor of exercise start and end dates at least three weeks in advance of exercise start date.

3.4.1 Contingency Support

Contractor shall provide Government as required with support during contingencies, including Alerts, Recalls, Emergency Response Drills, and Declared National Emergencies. Alerts and Recalls usually last one day. Emergency Response Drills and Declared National Emergencies will by their nature be of undetermined length.

3.4.1.2 Report-for-Duty Requirement

Contractor shall have sufficient number of employees on location to support contingency requirements NLT one hour after notification.

3.4.1.3 Contingency Support Requirement

Customer may require Contractor to support any or all networks, systems, and services.

3.4.1.4 On-Call Duty Roster

Contractor shall provide Government Technical Supervisor with 24 hour on-call roster (contact information) at contract start date and NLT five working days prior to expiration of current roster.

**3.5 Electronic and Information Technology (EIT) Information**.

All EIT information procured through this contract must meet applicable accessibility standards.

**3.6 IT Services**

Contractor shall provide C4i Customers with responsive, flexible IT services involving all IT areas applicable to this contract IAW Information Technology Infrastructure Library (ITIL) best business practices to the highest degree possible within the framework of each Customer's service delivery system. Contractor shall develop and implement efficient and effective standardized operating procedures (SOPs) {CDRL D008}. Contractor shall submit each SOP to Customer for approval NLT 30 days after contract start date and thereafter, whenever requested. In case of

conflict between a Contractor SOP and a Customer SOP, the Customer SOP holds precedence.

**3.7 Service Center Support**

3.7.1 Technical Support

Technical personnel shall provide C4i Customers with expert Tier-1 and Tier-2 C4i system and tactical network troubleshooting service, authorized service interruption (ASI) management, and security incident response. Contractor shall document service delivery procedures in Technical Support SOP.

3.7.1.2 Technical Support Personnel Technical Qualifications

In addition to meeting requirements identified in 3.5.5.4 "Contractor Technical Qualifications" paragraph, Contractor shall ensure that each Telecommunications Specialist (96) is at least Information Assurance Technical (IAT) Level II-certified.

3.7.1.3 Technical Support Personnel Language Requirements

Contractor shall ensure that Technical Support personnel are proficient at speaking English.

3.7.1.4 Technical Support Telephone Support

Technical Support personnel shall provide C4i Customers with prompt telephone support.

3.7.1.5 Technical Support Requirements

Contractor shall adhere to the following Technical Support procedures for General Officer (GO), Priority-1, Priority-2, Priority-3, and Priority-4 trouble tickets.

**3.7.1.6 Technical Support Trouble Ticket Priorities**

3.7.1.6.1 General Officer (GO) Trouble Tickets

Critical Impact: A request for direct GO support. This category includes trouble tickets affecting Senior Executive

Service (SES) civilians.

3.7.1.6.2 Priority-1 Trouble Tickets

Emergency or major outage: Service interruption that affects a major command center (e.g., CP Oscar, 8A Main), a large group of users, or a user identified on the current VIP List. Government will provide Contractor with initial VIP List and updated lists as changes are made.

3.7.1.6.3 Priority-2 Trouble Tickets

High-impact incident: A problem with no known work-around that impacts a single staff principal or commander

(COL/O-6).

3.7.1.6.4 Priority-3 Trouble Tickets. Medium-impact incident. A problem with no known work-around that impacts a single user.

3.7.1.6.5 Priority-4 Trouble Tickets. Routine incident: A general service problem with known work-around or a service request that does not require immediate attention or long-term planning.

**3..1.7 Technical Support Initial Response Requirements**

3..1.7.1 GO Trouble Ticket Initial Response Requirement. Contractor shall attempt to make initial contact with all GO/SES Customers (or their representatives) NLT 30 minutes after Technical Support’s initial receipt of trouble ticket.

3.7.1.7.2 Priority-1 Trouble Ticket Initial Response Requirement. Contractor shall attempt to make initial contact with all Priority-1 Customers NLT one hour after Technical Support’s initial receipt of trouble ticket.

3.7.1.7.3 Priority-2 Trouble Ticket Initial Response Requirement. Contractor shall attempt to make initial contact with all Priority-2 Customers NLT one duty hour after Technical Support’s initial receipt of trouble ticket.

3.7.1.7.4 Priority-3 Trouble Ticket Initial Response Requirement. Contractor shall attempt to make initial contact with all Priority-3 Customers NLT one duty hour after Technical Support’s initial receipt of trouble ticket.

3.7.1.7.5 Priority-4 Trouble Ticket Initial Response Requirement. Contractor shall attempt to make initial contact with all Priority-4 Customers NLT one duty hour after Technical Support’s initial receipt of trouble ticket.

**3.7.1.8 Technical Support Troubleshooting Support**

3.7.1.8.1 Technical Support Troubleshooting Responsibilities. Technical Support personnel shall provide Customers with Tier-1 and Tier-2 C4i system and tactical network troubleshooting service via secure telephone, non-secure telephone, and/or Government-designated remote desktop application.

**3.7.1.8.2 Technical Support Restoral Objectives**

3.7.1.8.2.1 GO Trouble Ticket Restoral Objective

Contractor shall resolve all GO C4i problems NLT 30 minutes after Technical Support’s initial receipt of trouble ticket.

3.7.1.8.2.2 Priority-1 Trouble Ticket Restoral Objective

Contractor shall resolve all Priority-1 IT problems NLT one hour after Technical Support’s initial receipt of trouble ticket.

3.7.1.8.2.3 Priority-2 Trouble Ticket Restoral Objective

Contractor shall resolve all Priority-2 IT problems NLT 24 duty hours after Technical Support’s initial receipt of trouble ticket.

3.7.1.8.2.4 Priority-3 Trouble Ticket Restoral Objective

Contractor shall resolve all Priority-3 IT problems NLT 48 duty hours after Technical Support’s initial receipt of trouble ticket.

3.7.1.8.2.5 Priority-4 Trouble Ticket Restoral Objective. Contractor shall resolve all Priority-4 IT problems NLT 72 duty hours after Technical Support’s initial receipt of trouble ticket.

3.7.1.8.2.6 Technical Support Escalation Procedures

Only applies to GO and Priority 1 trouble tickets. If Contractor does not attain a satisfactory response or resolution to a service outage or incident, Contractor shall notify Customer management personnel IAW the following escalation procedures.

3.7.1.8.2.7 Fifteen Minute GO/Priority-1 Trouble Ticket Outage

After 15 minutes of outage, Contractor shall escalate to 8A’s Network Operations and Headquarters’ Support

Division Chiefs.

3.7.1.8.2.8 Twenty Minute GO/Priority-1 Trouble Ticket Outage

After 20 minutes of outage, Contractor shall escalate to 8A G6 Operations Chief.

3.7.1.8.2.9 Thirty Minute GO/Priority-1 Trouble Ticket Outage

After 30 minutes of outage, Contractor shall escalate to 8A G6.

**3.7.1.9 Trouble Ticket Documentation Procedures**

3.7.1.9.1 Trouble Ticket Logging

Contractor shall record details of each service outage and incident reported to the Technical Support Center in a

Government-designated trouble ticket management system application.

3.7.1.9.2 Trouble Ticket Closure

Contractor shall keep each trouble ticket open until Customer verifies resolution.

3.7.1.9.3 Trouble Ticket Customer Satisfaction Survey

Upon closure of each trouble ticket, Contractor shall offer Customer the chance to complete a Government- developed Customer Satisfaction Survey.

3.7.1.9.3.1 Trouble Ticket Customer Satisfaction Survey Database

Contractor shall store all Trouble Ticket Customer Satisfaction data and comments in a database.

3.7.1.9.3.2 Trouble Ticket Customer Satisfaction Survey Reporting

Contractor shall report Trouble Ticket Customer Satisfaction figures to Government monthly. Customer dissatisfaction must not reach or exceed 3% of trouble tickets processed per month.

3.7.1.9.4 Trouble Ticket Metrics Reporting

Contractor shall report Trouble Ticket Metrics figures to Government monthly. Contractor shall include in each report, at a minimum, total number of trouble tickets processed and numbers and percentages that did and did not meet objectives for initial response, escalation, and restoral; those same figures broken out by priority; and graphs of all of those figures compared to same metrics during each of the previous 12 months. Contractor shall include narratives in the report to explain each of the previous month's unmet objectives for each trouble ticket.

3.7.1.9.5 Account Administration

Contractor shall document all account creation and maintenance actions in Government-designated trouble-ticket management system.

3.7.1.9.5.1 Account Creation

Contractor shall process account applications for new users after review by the Government. Contractor shall ensure that all applications for new user accounts indicate that the new user has met all Army IA training requirements and completed an acceptable use policy before processing account request.

3.7.1.9.5.2 Account Maintenance

Contractor shall perform maintenance on accounts for existing users. Maintenance activities may include password resets, profile edits, and account deletions. Contractor shall enforce Designated Accrediting Authority (DAA) user ID/password policy.

**3.7.2 C4i System Support.**

When called upon by the Technical Support Center, C4i System Support personnel shall provide C4i Customers with expert Tier-1 and Tier-2 C4i system and tactical network troubleshooting service and security incident response. Contractor shall document service delivery procedures in C4i System Support SOP.

3.7.2.1.2 C4i System Support Personnel Technical Qualifications

In addition to meeting requirements identified in "Contractor Technical Qualifications" paragraph, Contractor shall ensure that all Telecommunications Specialists (96) are at least IAT Level II-certified.

3.7.2.1.3 C4i System Support Personnel Language Requirements

Contractor shall ensure that all C4i System Support employees are proficient at speaking English.

3.7.2.2 C4i System Troubleshooting Support

When called upon by the Technical Support Center, C4i System Support personnel shall provide C4i Customers with expert Tier-1 and Tier-2 C4i system and tactical network troubleshooting service in order to help them resolve IT problems. Contractor shall adhere to the following C4i System Support procedures for General Officer (GO), Priority-1, Priority-2, Priority-3, and Priority-4 trouble tickets.

3.7.2.2.1 C4i System Trouble Tickets. See "Technical Support Trouble Ticket Priorities" paragraph.

3.7.2.2.2 C4i System Support Initial Response Requirements. See "Technical Initial Response Requirements" paragraph.

3.7.2.2.3 C4i System Support Troubleshooting Procedures

C4i System Support personnel shall provide Customers with expert Tier-1 and Tier-2 C4i system and tactical network troubleshooting service through secure telephone, non-secure telephone, Government-designated remote desktop application, and/or personal desk-side assistance.

3.7.2.2.4 C4i System Support Restoral Objectives. See 3.10.1.8.2 "Technical Support

Restoral Objectives" paragraph.

3.7.2.2.5 C4i System Support Escalation Procedures. See 3.10.1.8.2.6 "Technical Support Escalation Procedures" paragraph.

3.7.2.2.6 C4i System Support Documentation Procedures

C4i System Support personnel shall record details of coordination and troubleshooting actions attempted and their results, and either pass them to the Technical or enter them directly into the Government-designated trouble ticket management system application.

3.7.2.3 C4i System Installation and Upgrade Support

C4i System Support personnel shall perform hardware and software installations and upgrades for C4i Customers.

3.7.2.4 C4i System Support to 8A

C4i System Support personnel shall provide 8A Customers with expert Tier-1 and Tier-2 C4i system and tactical network, logical and physical, configuration, troubleshooting, and computer network defense services.

**3.7.3 Tactical Network Support**

When called upon by the Technical Support Center, Tactical Network Support personnel shall provide C4i Customers with expert tactical network troubleshooting service, security incident response, and network infrastructure installation and upgrade service. Contractor shall document service delivery procedures in Tactical Network Support SOP.

3.7.3.1.2 Tactical Network Personnel Technical Qualifications

In addition to meeting requirements identified in "Contractor Technical Qualifications" paragraph, Contractor shall ensure that all Telecommunication Specialists, Senior (97) is Information Assurance Technical (IAT) Level III- certified. Contractor shall ensure that Telecommunication Specialists (96) are at least IAT Level II-certified.

3.7.3.1.3 Tactical Network Personnel Language Requirements

Contractor shall ensure that at Tactical Network Support employees are proficient at speaking English. 3.10.3.1.4

Tactical Network Support Requirements and Standards. Contractor shall complete all Tactical Network Service

work IAW Customer’s officially documented specific requirements and all applicable DoD and Federal Government standards, including physical and network security standards (e.g., PDS, TEMPEST, COMSEC, and OPSEC).

3.7.3.2 Tactical Network Infrastructure Installations and Upgrades

Contractor shall perform complete all engineering, integration, and project management requirements for all funded projects involving new and/or additional tactical network infrastructure installations and upgrades.

3.7.3.2.1 Tactical Network Infrastructure Installations

Contractor shall complete all engineering, integration, and project management requirements for all funded projects involving new and/or additional tactical network infrastructure installations.

3.7.3.2.2 Tactical Network Infrastructure Upgrades

Contractor shall complete all engineering, integration, and project management requirements for all funded projects involving tactical network infrastructure upgrades. Contractor shall coordinate for all infrastructure parts and communications devices for all funded projects IAW warranty requirements, lifecycle requirements, and service delivery obligations related to other contracts.

3.7.3.2.3 Tactical Network Infrastructure Fast-track Requirements

8A G6 may authorize a tactical network infrastructure requirement to be put on the fast track. Contractor shall accelerate completion of all fast-track tactical network infrastructure requirements for all funded projects involving new and/or additional tactical network infrastructure.

3.7.3.3 Tactical Network Service Troubleshooting Support

Contractor shall adhere to the following Tactical Network Troubleshooting Support procedures for General Officer

(GO), Priority-1, Priority-2, Priority-3, and Priority-4 trouble tickets.

3.7.3.3.1 Tactical Network Service Trouble Tickets. See "Technical Support Trouble Ticket Priorities" paragraph.

3.7.3.3.2 Tactical Network Service Response Requirements. See "Technical Support Initial Response Requirements" paragraph.

3.7.3.3.3 Tactical Network Service Troubleshooting Procedures

Tactical Network Service Troubleshooting Support personnel shall provide Customers with expert Tactical Network troubleshooting service via secure telephone, non-secure telephone, Government-designated remote desktop application, personal desk-side assistance, and/or vendor support acquisition.

3.7.3.3.4 Tactical Network Service Restoral Objectives. See 3.10.1.8.2 “Technical Restoral Objectives" paragraph.

3.7.3.3.5 Tactical Network Service Escalation Procedures. See 3.10.1.8.2.6 “Technical Escalation Procedures" paragraph.

3.7.3.3.6 Tactical Network Service Documentation Procedures

Tactical Network Service Troubleshooting Support personnel shall record details of coordination and troubleshooting actions attempted and their results, and either pass them to the Technical Support Center, or enter them directly into the Government-designated trouble ticket management system application.

**3.7.4 Tactical Network Engineering Support**

Contractor shall provide C4i Customers with tactical network troubleshooting service, security incident response, and tactical network infrastructure advanced engineering support. Contractor shall document service delivery procedures in Tactical Network Engineering Support SOP.

3.7.4.2 C4i Systems Architecture, Planning, and Engineering Support

Contractor shall provide Customer with Systems Architecture, Planning, and Engineering support.

3.7.4.2.1 C4i Systems Architecture, Planning, and Engineering Support Technical Qualifications

In addition to meeting requirements identified in 3.5.5.4 "Contractor Technical Qualifications" paragraph, Contractor shall ensure that all Senior INFOSEC Engineer (149) support personnel are at least IA Workforce System Architect and Engineer (IASAE) Level III-certified.

3.7.4.2 C4i Systems Architecture, Planning, and Engineering Support Responsibilities.

Contractor shall interface with Customer and organizations to research and analyze operational and technical system information, and use that information to develop support documents, including analysis, assessment, report, staff package, briefing, meeting, and in-progress review (IPR) documents.

**3.8 Operations and Maintenance**

3.8.1 C4i System Administration

Contractor shall provide all tactical C4i System Administration services, including authentication, messaging, application, collaboration, data storage, file/print, anti-virus, Windows update, and back-up and recovery services. Contractor shall document service delivery procedures in C4i System Administration SOP.

3.8.1.1.3 C4i System Administration Support Personnel Technical Qualifications

In addition to meeting requirements identified in "Contractor Technical Qualifications" paragraph, Contractor shall ensure that all Telecommunication Specialists (96) personnel are at least IAT Level II-certified.

3.8.1.1.4 C2 Authentication Services

Contractor shall provide authentication services on US-Unclassified and US-Secret Tactical Communications networks. C4I authentication services currently include Domain Controller, Active Directory, and Group Policy services.

3.8.1.2 C4i Tactical Messaging Services

Contractor shall provide messaging services on US-Unclassified and US-Secret Tactical Communications networks. C4I messaging services currently include Exchange and Chat services.

3.8.1.3 C4i Application Services

Contractor shall provide C2 services on US-Unclassified and US-Secret Tactical Communications networks.

3.8.1.4 C4i Collaboration Services

Contractor shall provide collaboration services on US-Unclassified and US-Secret Tactical Communications networks. C4I collaboration services currently include Portal Collaboration, Desktop Conferencing, Whiteboard, and Video/Audio Presentation services.

3.8.1.5 C4i Data Storage Services

Contractor shall provide data storage services on US-Unclassified and US-Secret Tactical Communications networks. C4I data storage services currently include data storage, storage area network (SAN) and network- attached storage (NAS) services.

3.8.1.6 C4i File/Print Services

Contractor shall provide file/print services on US-Unclassified and US-Secret Tactical Communications networks.

3.8.1.7 C4i Anti-Virus Services

Contractor shall provide anti-virus services on US-Unclassified and US-Secret Tactical Communications networks.

3.8.1.8 C4i Windows Update Services

Contractor shall push all critical Windows Updates to the tactical enterprise within 48 hours of release.

**3.8.2 Tactical Network Administration**

Contractor shall document service delivery procedures in Tactical Network Administration SOP.

3.8.2.1.2 Tactical Network Administration Support Personnel Technical Qualifications.

In addition to meeting requirements identified in "Contractor Technical Qualifications" paragraph, Contractor shall ensure that all Telecommunication Specialists (96) personnel are at least IAT Level II-certified.

3.8.2.2 C4i Network WAN Links

Contractor shall provide circuit availability IAW official Government guidelines, which currently includes the DISA Telecommunications Service Priority (TSP) assigned to the Control Communications Service Designator (CCSD) of each circuit supporting the network.

3.8.2.3 C4i Tactical Network Equipment Configuration

Maintain tactical network equipment configurations IAW official Government guidelines, which currently include

Government-approved engineering solutions and Security Technical Implementation Guides (STIGs).

3.8.2.4 C4i Network Access Control (NAC)

Contractor shall provide tactical network access hardware and software. Ensure tactical network access is restricted to Designated Accrediting Authority (DAA)-approved individuals and accomplished IAW official Government guidelines, which currently include Security Technical Implementation Guides (STIGs).

3.8.2.5 C4i Tactical Network Device Configuration Data

Maintain tactical network device configuration hardware, software, and data. Ensure configurations are stored as baseline controlled items IAW official Government guidelines, which currently include Security Technical Implementation Guides (STIGs).

3.8.2.6 C4I Tactical Network Events

Maintain tactical network event hardware, software, and data. Ensure tactical network devices deliver log event data to a centralized, managed device where they are reported, logged, and archived IAW official Government

guidelines, which currently include Security Technical Implementation Guides (STIGs).

**3.8.3 Tactical Real-time Services**

Contractor shall provide all C4I tactical real-time services, including Voice over Internet Protocol (VoIP), Voce over Secure Internet Protocol (VoSIP), video teleconferencing (VTC), and video streaming. Contractor shall document service delivery procedures in Tactical Real-time Services SOP.

3.8.3.1.2 Tactical Real-time Services Support Personnel Technical Qualifications

In addition to meeting requirements identified in "Contractor Technical Qualifications" paragraph, Contractor shall ensure that all Telecommunication Specialists (96) personnel are at least IAT Level II-certified.

3.8.3.2 Voice over Internet Protocol (VoIP) Support

Contractor shall provide 99.8% availability of VoIP services.

3.8.3.3 Voice over Secure Internet Protocol (VoSIP) Support

Contractor shall provide of VoSIP services.

3.8.3.4 Video Teleconferencing (VTC) Support

Contractor shall provide VTC services on 8A-owned VTC systems.

3.8.3.5 Video Streaming Support

Contractor shall provide video streaming services.

3.8.3.6 Video Wall Maintenance Support

Contractor shall provide on-site C4I Video Wall Maintenance support IAW best business practices.

3.8.3.6.1 Video Wall Maintenance Program

Contractor shall implement a maintenance program that covers on-site Video Wall technical support.

3.8.3.6.2 Video Wall Preventive Maintenance

Contractor shall perform preventive maintenance inspections (PMIs) quarterly on all Video Wall systems.

3.8.3.7 Video Wall Demand Maintenance.

3.8.3.7.1 Video Wall Tier-1 On-Site Demand Maintenance

During normal operations, Contractor shall respond on-site to Tier-1 incidents within six hours; during major exercises, within two hours.

3.8.3.7.2 Video Wall Tier-2 On-Site Demand Maintenance

During normal operations, Contractor shall respond on-site to Tier-2 incidents within 24 hours; during major exercises, within four hours.

3.8.3.8 Video Wall Repair Parts and Consumables.

3.8.3.8.1 Video Wall Tier-1 Site Repair Parts

Government will maintain and replenish a common pool of repair parts and consumables and allocate items to Contractor as needed. Contractor shall manage inventories and provide Government with monthly reports which will include current stock levels and projected stock requirements.

3.8.3.8.2 Video Wall Tier-2 Site Repair Parts

Government will manage spare parts and consumables.

**3.9 DoD Information Assurance**

Contractor shall perform the following information assurance support tasks:

3.9.1 Ensure 8A personnel are registered in the Army Training and Certification database (ATCTS). Coordinate with 8A MSCs and staff to ensure proper management and reporting within ATCTS. Provide reports on a monthly basis. Generate and provide training and certification status of 8A personnel in a timely manner to include but not limited to writing scripts to generate accurate and time sensitive reports.

3.9.2 Ensure 8A systems are registered and maintained in the Army Portfolio Management System (APMS). Ensure system owners update required FISMA data and report status of 8A systems on a monthly basis.

3.9.3 Ensure 8A systems are registered in the Army certification and accreditation database (C&A Tdb). Coordinate with system owners to ensure timely and adequate progress towards accreditation/reaccreditation. Report status of accreditations of 8A systems on a monthly basis.

3.9.4 Provide knowledge management for the IA Share point site and update as needed.

3.9.5 Provide technical support and assistance for IA staff inspections and assistance visits of 8A Major Subordinate Commands (MSCs) and Staff. Provide technical reports and staff inspection products. Maintain IA checklist, track required changes throughout the year, and update annually NLT 30 JUN.

3.9.6 Create, maintain, and update 8A IA Division Standard Operating Procedures (SOP) to include, but not limited to, continuity books and other SOPs as needed.

3.9.7 Prepare staffing products to include, but not limited to OPORDs/FRAGOs, policies, briefings (PowerPoint), white papers, and information papers IAW 8A standards

3.9 8 Maintain cyber-watch lists. Check for new tasking orders, OPORDs from higher HQs, Best Business Practices

(BBP), policies, and directives. Develop courses of actions and recommendations for 8A.

3.9.9 Keep abreast of DoD-approved system security tools, IA tools, and products. Develop recommendations and implementation plan if tool can benefit 8A.

3.9.10 Attend meetings to represent 8A and provide input as required. Provide written information paper of the discussions NLT 2 business days after the meeting.

3.9.11 Support 8A exercises and deploy to exercise locations within the Pacific or elsewhere when mission requires.

3.9.12 Coordinate with Department of Army (DA) or other government agencies such as Army Test and Evaluation Command (ATEC) and DISA for Command Cyber Readiness Inspection (CCRI), Department of Army Inspector General (DAIG) inspection, or ACAs. Develop plans and draft orders to prepare for successful execution of inspections/certification events within 8A.

3.9.13 Assist 8A MSCs and Staff for any IA related issues to include but not limited to Certification and

Accreditation (C&A) and Training and Certification (T&C).

3.9.14 Coordinate IA training for 8A throughout Korea and perform necessary coordination/tasks to ensure successful attendance and completion.

3.9.15 Maintain IA group email boxes for administrative functions and check for IA related messages. Continuously update IA distribution lists on US-Unclassified, US-Secret, and CENTRIXS-K networks to ensure most up-to-date POCs are maintained.

3.9.16 Adhere to and advise on IA policies and regulations, BBP, IA guidance and directives to support 8A.

3.9.17 Use IA tools provided by government to evaluate security of 8A systems and assist 8A MSCs and Staff to fix vulnerabilities/issues found. Create and maintain SOP on how to use the tools.

3.9.18 Obtain and maintain IA baseline certification at the IA Management Level II and IA Technical Level II, per

DoD Instruction 8570.01-M.

3.9.19 Obtain and maintain SECRET clearance.

3.9.20 Command Cyber Readiness Inspection (CCRI) Compliance. Contractor shall comply with all CCRI policies in order to pass all CCRIs and remediate and report all deficiencies found during CCRIs.

3.9.21 Obtain and maintain IA baseline certification at the Computer Network Defense-Service Provider (CND-SP) Analyst, Infrastructure Support, Incident Responder, or Auditor per DoD Instruction 8570.01-M.

**3.10 Training Services**

Contractor shall provide C4i Customers, expert Training support. Contractor shall provide formal instructor-led and/or computer-based training for all US-Unclassified and US-Secret network/system users and the Information Management Officers (IMOs) who serve them.

3.10.1 Software Application and System Training

Contractor shall provide training on C4i software applications and systems (e.g. SharePoint).

3.10.2 Hardware Equipment and System Training

Contractor shall provide training on C4i hardware equipment and systems, including COMSEC, VTC, and network items.

**3.11 Management Services**

Contractor shall provide C4i Customers with responsive, flexible Management support on issues relating to personnel, coordination, logistics, maintenance, vehicle management, performance, quality control, Contract Funds Status Report, Contract Work Breakdown Structure, Integrated Master Schedule (IMS), and evaluation issues. Contractor shall participate in Integrated Process Teams (IPTs) and other technical and management meetings and reviews, as required by Government, to assist with planning for, integrating, and installing engineering solutions. Contractor shall develop and implement efficient and effective standardized operating procedures (SOPs). Contractor shall submit each SOP to Customer for approval NLT 30 days after contract start date and thereafter, whenever requested.

3.11.1 Management Support Personnel Requirements

Contractor shall provide C4i Customers with expert Management support.

**3.11.1 Resource Administrative Management Support**

Contractor shall provide expert, responsive, and flexible resource administrative management support on issues relating to high quality project support, maintenance of logs, records, archives, and other working files, preparation of reports and meeting/travel arrangements applicable to task execution.

**3.11.2 Technical Management Support**

Contractor shall provide Customers with baseline configuration and topology information and other technical information (in the form of written technical papers and staff papers) pertaining to C4i systems to support: Contractor shall document management support procedures in Technical Management Support SOP.

3.11.2.1 Integrated Process Team (IPT) Support

Contractor shall participate in Integrated Process Teams (IPTs) and other technical and management meetings and reviews, as required by the Government, to assist with planning for, integrating and installing Engineering Solutions which are developed under this task.

3.11.2.2 Immediate Priority Work Reporting

Contractor shall provide Government with written reports {CDRL D011} (e-mails, information papers, briefings, or technical data), as required, on the status of Immediate Priority tasking.

3.11.2.3 Associated Contract Support

Contractor shall support and coordinate work with other contractors who are performing tasks in support of this contract's Customers, including developing engineering solutions, resolving configuration and security issues, and accomplishing Certification and Accreditation processes.

3.11.2.4 Metrics Report

Contractor shall provide Government with a monthly Metrics Report NLT the tenth working day of the next month that compares Contractor’s performance figures to standards established in this contract’s Performance-based Work Statement (PWS), Performance Requirements Summary (PRS) and Quality Assurance Surveillance Plan (QASP).

3.11.3 Environmental Maintenance Support

Contractor shall provide on-site environmental maintenance support at major 8A locations.

3.11.3.1 Heating, Ventilating, and Air Conditioning (HVAC). Contractor shall coordinate, schedule and arrange

HVAC and standby generator support from DPW.

3.11.3.2 Uninterruptible Power Supply (UPS). Contractor shall coordinate, schedule and arrange UPS maintenance support from the vendor.

**3.12 Antiterrorism/OPSEC Requirements**

**3.12.1 AT Level 1 Training**

All contractor employees, to include subcontractor employees, requiring access Army installations, facilities and controlled access areas shall complete AT Level I awareness training within 30 calendar days after contract start date or effective date of incorporation of this requirement into the contract, whichever is applicable. The contractor shall submit certificates of completion for each affected contractor employee and subcontractor employee, to the COR or to the contracting officer, if a COR is not assigned, within 30 calendar days after completion of training by all employees and subcontractor personnel. AT level I awareness training is available at the following website: https://atlevel1.dtic.mil/at.

**3.13 Access and General Protection/Security Policy and Procedures**

Contractor and all associated sub-contractors employees with an area of performance within an Army controlled installation, facility or area, shall comply with applicable installation, facility and area commander installation/facility access and local security policies and procedures (provided by government representative). The contractor shall also provide all information required for background checks to meet installation access requirements to be accomplished by installation Provost Marshal Office, Director of Emergency Services or Security Office. Contractor workforce must comply with all personal identity verification requirements as directed by DOD, HQDA and/or local policy. In addition to the changes otherwise authorized by the changes clause of this contract, should the Force Protection Condition (FPCON) at any individual facility or installation change, the Government may require changes in contractor security matters or processes.

**3.14 iWATCH Training**

Contractor and all associated sub-contractors with an area of performance within an Army controlled installation, facility or area, shall brief all employees on the local iWATCH program (training standards provided by the requiring activity ATO). This local developed training will be used to inform employees of the types of behavior to watch for and instruct employees to report suspicious activity to the COR. This training shall be completed within

30 calendar days of contract award and within 30 calendar days of new employees commencing performance with the results reported to the COR NLT 30 calendar days after contract award.

**3.15 Access to Government Information Systems**

All contractor employees with access to a government info system must be registered in the ATCTS (Army Training Certification Tracking System) at commencement of services, and must successfully complete the DOD Information Assurance Awareness prior to access to the IS and then annually thereafter.

**3.16 OPSEC Training**

Per AR 530-1, Operations Security, new contractor employees must complete Level I OPSEC training within 30 calendar days of their reporting for duty. All contractor employees must complete annual OPSEC awareness training.

**3.17 Information Assurance (IA)/Information Technology (IT) Training**

All contractor employees and associated sub-contractor employees must complete the DoD IA awareness training before issuance of network access and annually thereafter. All contractor employees working IA/IT functions must comply with DoD and Army training requirements in DoDD 8570.01, DoD 8570.01-M and AR 25-2 within six months of employment.

**3.18 Information Assurance (IA)/Information Technology (IT) Certification**

Per DoD 8570.01-M , DFARS 252.239.7001 and AR 25-2, the contractor employees supporting IA/IT functions shall be appropriately certified upon contract award. The baseline certification as stipulated in DoD 8570.01-M must be completed upon contract award.

**3.19 Performance or Delivery in a Foreign Country**

DFARS Clause 252.225-7043, Antiterrorism/Force Protection for Defense Contractors Outside the US, shall be used in solicitations and contracts that require performance or delivery in a foreign country. This clause applies to both contingencies and non-contingency support. The key AT requirement is for non-local national contractor personnel to comply with theater clearance requirements and allows the combatant commander to exercise oversight to ensure the contractor’s compliance with combatant commander and subordinate task force commander policies and directives.

**3.20 Handling or Access to Classified Information**

Contractor shall comply with FAR 52.204-2, Security Requirements. This clause involves access to information classified “Confidential,” “Secret,” or “Top Secret” and requires contractors to comply with— (1) The Security Agreement (DD Form 441), including the National Industrial Security Program Operating Manual (DoD 5220.22- M); any revisions to DOD 5220.22-M, notice of which has been furnished to the contractor.

**4.0 TRAVEL**

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 whether travel costs are reasonable. 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 reviewed in advance by the COR.

**5.0 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 without explicit authorization of a relevant Government official, and that is based on a need-to- know basis only. Individuals getting access must have the appropriate clearance for access to a particular system.