PERFORMANCE WORK STATEMENT

FOR ARMY ENTERPRISE IT SERVICES, PLANNING AND ENGINEERING

IN SUPPORT OF THE

NETWORK ENTERPRISE TECHNOLOGY COMMAND

TABLE OF CONTENTS

C.1.0. SCOPE

The Contractor shall provide non-personal Army Enterprise Internet Protocol Video TeleConference (IP-VTC) services supporting the United States Army Network Enterprise Technology Command (NETCOM). Contractor support will primarily be required in the NETCOM Headquarters, subcommand organizations and other NETCOM supported locations as defined in the DD254. The Contractor shall provide IT support to NETCOM and NETCOM supported organizations for Department of Defense (DoD) Information Network (DoDIN) hardware, software, data, applications, tools, and systems used/provided by the Army. The Contractor shall provide direct support to the NETCOM and its worldwide customers with business operations, Network Operations (NetOps), Operations and Maintenance (O&M) support, Cybersecurity, Knowledge Management (KM), Army Enterprise Service Ownership/Development and Capability Management, plus Content Management requirements for Army Enterprise IP-VTC capabilities and services. The Contractor shall provide support in accordance with (IAW) industry and Army/DoD best practices as delineated in frameworks/guidelines such as the Information Technology Infrastructure Library (ITIL), Army Enterprise Service Management Framework (AESMF), DoD Enterprise Service Management Framework (DESMF), and Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs). Contractor support is required in the NETCOM managed Department of Defense Information Network - Army (DoDIN- Army) Nonsecure Internet Protocol Router Network (NIPRNET) and Secure Internet Protocol Router Network (SIPRNET) environments.

C.2.0. BACKGROUND

NETCOM is the Army Enterprise's DoDIN operations and services provider, executing full-spectrum cyber operations to attain information superiority and achieve an integrated network enterprise across the Joint, Interagency, Intergovernmental, and Multinational (JIIM) domains. NETCOM plans, engineers, installs, integrates, operates, protects, maintains, and sustains the Army Cyberspace domain, thus enabling Mission Command through all phases of unified action operations with all mission partners across the JIIM domains. NETCOM designs, implements, operates, and manages several Army Enterprise services/capabilities such as Army Enterprise SharePoint Service (AES2), Internet Protocol Video Teleconference (IP-VTC), and Enterprise Collaboration Services (ECS). Some of these capabilities are provisioned as (or supported by) a DISA provided and managed service, as in the case of ECS, or as a mix of DISA managed service and NETCOM operations and management, as with Global Video Services (GVS) in support of IP-VTC. NETCOM is the single authority assigned to operate, manage, and defend the Army's "InfoStructure" at the enterprise level and the single authority for any standard, system, architecture, design, or device that impacts the Army Enterprise Infostructure that comprises the DoDIN-Army.

C.3.0. FUNCTIONAL PERFORMANCE REQUIREMENTS

The Contractor shall provide services with various types of necessary IT experience, including operational and technical capability management, strategic and technical capability development, project integration, process development, Information Assurance (IA), configuration management (CM), hardware/software support, as well as support functions such as database policy definition, requirements development and management, and technical writing. When working with non-NETCOM stakeholders, the Contractor shall ensure that all personnel understand the Contractor's status as a non-Government employee. When working with non-NETCOM organizations, the Contractor shall not obligate or bind the Government in any way, enter into any agreements on the Government's behalf, or

exercise any Governmental discretion. The Contractor shall only articulate NETCOM's positions and policies and provide technical information IAW Government direction.

The Contractor shall provide support for Unified Capabilities. The Army defines Unified Capabilities as the integration of Voice, Video, and Data services delivered ubiquitously across a secure and highly available infrastructure, independent of the technology, to provide increased mission effectiveness to the Warfighter and business communities. For the purpose of this contract, Unified Capabilities includes Internet Protocol – Video Telecommunications (IP-VTC), Voice over Internet Protocol (VOIP), and Instant Messaging and Collaborative Services. These are described in the following four functional areas:

C.3.1. Army Enterprise Service Ownership and Development, the Contractor shall:
Support the NETCOM IP-VTC Capability Manager in the long-term strategic development, production, delivery, and execution of enterprise services provided, by NETCOM IP-VTC, to our customers and supported commands, as developed and laid out in the Command Control Communications Computers and Information Management (C4IM) Services List and LandWarNet (LWN) Services Catalog, from initial development through LifeCycle Management (LCM) to service retirement. Assist the Capability Manager with planning and implementing continual improvements and change management; underlying processes that support/enable the enterprise service/capability; managing the end-to-end lifecycle of services and systems, including service deployment and lifecycle management (LCM) schedules; developing the Service Design Package and System Design Plan; preparing Service Support Modules (SSMs); and implementing approved changes to services throughout the Army Enterprise. Supports the Capability Manager in providing the enterprise services outlined in the supported organization's individual Service Level Agreements (SLAs).

- The Contractor shall assist the Government with cybersecurity functional support for assessments, authorizations, and documentation of enterprise fielded systems managed by NETCOM HQ.

- The Contractor shall provide qualified and cleared personnel to support NETCOM with its Risk Management Framework (RMF) processes.

- These efforts include utilizing the Enterprise Mission Assurance Support Service (eMASS) to record RMF activities such as control implementation of all applicable Security Controls as identified via information system security categorization in accordance with NIST SP 800-53 and CNSSI 1253 (security controls are broken down into individual, measureable, statements called assessment procedures or Control Correlation Indicators (CCIs)) in accordance with DoDI 8510.01 (Risk Management Framework (RMF) for DoD Information Technology (IT)). The number of families and controls will vary depending on the security categorization (C-I-A), the application of overlays (privacy, classified, intel, etc.) and any security control tailoring.

- The contractor will assist the Government Capability Manager / Information System Owner (ISO) in ensuring that the information systems are configured in accordance with DISA Security Technical Implementation Guides (STIGs), applicable patches and other cybersecurity requirements.

- The Contractor shall support the Government in following the DoD cybersecurity policy requirements set forth in DoDI 8500.01, "Cybersecurity," and DoDI 8510.01, "Risk Management Framework (RMF) for DoD Information Technology (IT)" and their successors.

- The Contractor shall provide support for the independent assessment of compliance of information systems with DoD RMF standards using DoDI 8510.01.

- The Contractor shall provide personnel with extensive experience with DoD security hardening, collection and assessment tools (STIGs, ACAS SCAP, Nessus, etc.) and experience with security architectures, firewalls and network access.

- The Contractor shall possess extensive experience in cybersecurity documentation and system authorization artifacts (System Security Plan, lifecycle documentation, continuous monitoring plan, Security Assessment Plan, Security Assessment Report, Risk Assessment, etc.).

- The Contractor shall have extensive knowledge of and review the Risk Management Framework (RMF) Knowledge Service - https://rmfks.osd.mil/rmf/Pages/default.aspx - which is the DoD's official site for enterprise RMF policy and implementation guidelines.

- The Contractor will review and ensure that any RMF activities on behalf of NETCOM adhere to the operational Tactics, Techniques and Procedures (TTPs) and Operations Orders that are hosted on the US Army Component Workspace – Operations tab of the RMF Knowledge Service. The TTPs provide amplifying guidance and process implementation for the Army regarding RMF.

- The contractor shall provide technical input on CoN submissions.

C.3.2. Army Enterprise Capability Management, the Contractor shall:
Assist the NETCOM CM in development of enterprise services/capabilities, including Army Portfolio Management System (APMS) system registration and maintenance, concepts of operations (CONOPS), functional requirements documents (FRD), Enterprise Technical Procedures (ETP), and Standard Operating Procedures (SOP), Change Configuration Release and Management (CCRM) Deployment Plan, doctrine, policies, processes, standards, and other supporting documentation. Support NETCOM CM in developing and supporting key solutions for service/capability implementation, fielding, and operations, including concepts, architecture, requirements, and integration (between operational, and strategic levels of operations) analysis for related solutions throughout the Army Enterprise; provide technical guidance for enterprise systems that affect the mission-essential operations of the DoDIN-Army; and coordinates with other Army Commands, installations, key personnel, and industry partners to develop and implement a plan to transition, migrate, and onboard organizations and their users. Provide information, analysis, and recommendations on the required force structure requirements (organization, training, and personnel), and changing roles and responsibilities associated with NetOps, migration, onboarding, and provisioning of tiered O&M support; and then implements those programs.

C.3.3. Army Enterprise Internet Protocol Video Teleconference (IP-VTC) Non-secure Internet Protocol Network (NIPRNET) and Secure Internet Protocol Network (SIPRNET) **Support Center (EVSC), the Contractor shall:**
Manage, monitor, secure, and sustain the enterprise VTC device registration hubs, call proxy and security boundary devices at 14 Regional Hub sites. The Contractor shall support IP VTC bridge

equipment strategically located to provide an Enterprise Army VTC meeting points and VTC bridge conferences services. The Contractor shall support Tier 0 or Top level VTC routing sites that allows seamless routing between Army and other agency VTC Call routing infrastructures. VTC users may scale up to 600,000 end users supported by 2018. The Contractor shall provide tier I (Basic user issues, general product and services, gather information, analyze symptoms), tier II (investigate issues raised from tier 1 support and check for known solutions to complex issues), and tier III (handles the most difficult problems and are experts in their field often conducts research and develops solutions for new or unknown issues) support for the NETCOM Headquarters and Regional Cyber Center (RCC) internal VTC equipment. The Contractor shall provide on-call support for Enterprise VTC systems 24 hours a day, seven days a week. During the life of this contract, some work associated with IP VTC management may be moved to higher echelons. The Contractor shall:

C.3.3.1 Provide VTC infrastructure device system administration support to CONUS and OCONUS Unified Communications (UC) systems, Operate, monitor, sustain, and secure VTC endpoints, IP VTC Proxy and security boundary devices, VTC device NetOps tools, and IP VTC bridges and conference data storage solutions.

C.3.3.2 Configure VTC client software on NIPRNet and SIPRNet to communicate with deployed users and DoD users in all military theater of operations.

C.3.3.3 Ensure the VTC equipment and applications are STIG and IAVA compliant.

C.3.3.4 Provide on call Tier III IP VTC support for Fort Gordon with an on-site contractor, Fort Eustis, Fort Sam Houston, Regional Cyber Center - Pacific, and Regional Cyber Center – Korea, 24 hours a day, seven days a week remotely during the first year and on-site labor during the following years. Provide Tier I, II, and III IP internal and enterprise VTC support at Fort Huachuca 24 hours a day, seven days a week.

C.3.3.4.1. Tier I, II, and III include providing VTC scheduling, call monitoring, endpoint testing, and troubleshooting support to NETCOM customers utilizing IP-VTC services.

C.3.3.4.2. Local On-Call touch labor support (TDY) to customers within the 7th Area of Responsibility (AOR) consisting of Ft Gordon, GA, Ft Eustis, VA, and Ft Sam Houston, TX, as needed.

C.3.3.4.3 Provide support for third party VTC interoperability, testing, and troubleshooting. This support includes Army customers using DISA's Global Video Service (GVS), independent Army owned Edge Border Controllers (EBCs) and VTC bridges, and external DoD VTC entities (Air Force, Navy, etc.)

C.3.3.5. Configure VTC call manager suites of equipment on NIPRNet and SIPRNet to communicate with call managers at the deployed unit locations and with call managers in all military theaters of operations.

C.3.3.6. Coordinate with installation RCCs and Network Enterprise Centers (NECs) to ensure network connectivity is available and alert NEC system administrators about outages.

C.3.3.7. Troubleshoot and monitor appliances for failures and alarms.

C.3.3.8. Notify affected installations at least 24 hours prior to scheduled outages or repairs to the management and database servers.

C.3.3.9. Install, configure, and maintain a lab environment in support of Information Assurance Vulnerability Alert (IAVA) testing/patches and system/database upgrades.

C.3.3.10. Provide technical guidance and support to end-users, sites, including posts, camps, and stations, on problems relating to the endpoints, bridges, VTC appliances, and Global Video Services (GVS).

C.3.3.11. Maintain accurate system diagrams and store them in a central location accessible only within NETCOM.

C.3.3.12. Provide timely situational awareness of critical events, their impact, reasons for outages, projected time to resolve, and final resolutions.

C.3.3.13. Report intrusions, suspected or actual security incidences to the Government Lead, Watch Officer, G2 Security Officer and follow local reporting Procedures.

C.3.3.14. Create administrative and user accounts.

C.3.3.15. Implement, create, delete, and maintain user permissions so that authorized client users can access servers and appliances.

C.3.3.16. Verify users' completion of SecureLogix Course or computer-based training (CBT) prior to issuing them accounts.

C.3.3.17. Maintain administrative accounts and renew expiring administrative passwords.

C.3.3.18. Enterprise Instant Messaging (IM) and Collaborative Services over IP on NIPRNET and SIPRNET. The Contractor will be prepared for the eventual installation of several real time communication services not currently prevalent such as:

C.3.3.18.1. Enterprise IM and collaborative services systems that do not currently exist at the Army Enterprise level. The Contractor shall be prepared to support an eventual Enterprise IM and Collaboration Tool systems to be determined at a later date. These systems may also be integrated with the existing Enterprise Voice over Internet Protocol (VoIP) and VTC Enterprise solutions for seamless call and communication routing, i.e. Jabber, Avaya, GenBand, Skype for Business, and Office 365.

C.3.4. Army Enterprise Unified Capabilities (UC) and Voice over Internet Protocol (VoIP), the Contractor shall:

C.3.4.1. The Contractor shall manage, monitor, secure, and sustain the Enterprise and theaters VOIP Edge/Session Border Controllers (EBC, SBC), Call Processing Managers and VoIP equipment. The equipment is being installed currently and into the future. Enterprise VoIP infrastructures will encompass all P/C/S and approximately 1.2M end users supported by 2020. The Contractor shall provide on-call support for VOIP 24 hours a day, seven days a week. The Contractor shall -

C3.4.2. Provide VOIP system administration support to CONUS and Pacific Theaters for Unified Communications (UC) systems, Operate, monitor, sustain, and secure VOIP technologies such as IP-PBX, IP telephony, VOIP handsets, call control managers, SBCs and EBCs. The SWA and European Theaters may be added at a later date, as mission dictates.

C.3.4.3. Configure call manager suites of equipment on NIPRNet and SIPRNet to communicate with call managers at the deployed unit locations and with call managers in all military theater of operations.

C.3.4.4. Ensure the UC equipment and applications are STIG compliant.

C.3.4.5. Provide Tier III IP VoIP support at Fort Gordon, Fort Eustis, and Fort Sam Houston in CONUS, at RCC-P and RCC-K in PACIFIC, and on call Tier III VoIP support 24 hours a day, seven days a week. Provide Tier I, II, and III IP internal and enterprise VoIP support at Fort Huachuca 24 hours a day, seven days a week.

C.3.4.6. Provide support to integrate together both VoIP and IP VTC infrastructures routing and call bridging functions so VoIP and VTC systems call seamlessly with one another.

C.3.4.7. Enterprise Instant Messaging (IM) and Collaborative Services over IP on NIPRNET and SIPRNET. The Contractor be prepared for the eventual installation of several real time communication services such as Enterprise IM and collaborative services systems that do not currently exist at the Army Enterprise level. Therefore the contractor should be prepared to support Enterprise IM and Collaboration Tool systems at a later date to be determined. These systems may also be integrated with the existing Enterprise VoIP and IP-VTC solutions for seamless call and communication routing.

C.4.0. COMMON SUPPORT PERFORMANCE REQUIREMENTS.
The Contractor shall perform these common support performance requirements in support of the individual capabilities found within this document:

C.4.1. Keep the COR apprised of any impacts to cost, schedule, and performance as the impact occurs.

C.4.2. Draft, modify and provide input for, the following documentation such as: white papers, diagrams, Concept of Operations (CONOPS), System Design Plans (SDP), Interim Authority to Test (IATT), Interim Authority to Operate (IATO), Authority to Operate (ATO), Certificate of Networthiness (CoN), Test Plans, Weekly Situational Reports (SITREP) and Enterprise Technical Procedures (ETP), Metalogix audits/reports, CA, projects, and applications.

C.4.3. Develop briefings, charts, technical papers, ad-hoc and recurring reports, spreadsheets, diagrams, In-progress reviews (IPRs) and other written documentation and graphical material.

C.4.4. Draft, maintain, provide input to and update technical documentation such as Service Design Plan (SDP), Engineering Implementation Plan (EIP), Software Acceptance test (SAT), ISSPs, Software Test Plan (STP), Software Implementation Plan (SIP), implementation guides, TTPs, and implementation plans.

C.4.5. Review, draft and provide technical input for Operations Orders (OPORDS), Fragmentary Orders (FRAGO), POAMs, Functional Requirements Document (FRD)s, TTPs, RFC, and other system requirements documentation per capability.

C.4.6. Work closely with SMEs and interface with IT management, specialists, and engineers throughout all echelons of the IT community to continuously improve processes.

C.4.7. Develop metrics tests, measures, artifacts, and analyze reports to determine process effectiveness and residual risks.

C.4.8. Analyze, diagnose and recommend improvements to complex processes. Provide technical advice and assistance to assigned projects and suggest efficient approaches and methods to resolve problems.

C.4.9. Identify applicable DoD, Army, and Federal Information Security Management Act requirements including but not limited to DoD IA controls, criticality, and threat. Assist the Government in validating capability requirements compliance.

C.4.10. Assess the supported unit's processes and draft recommended changes for updates.

C.4.11. Review existing documentation and processes as well as draft new documentation to ensure accurate detail of the implementation requirements.

C.4.12. Draft implementation guidance, best practice information and detailed specifications of supported activities.

C.4.13 Coordinate information exchanges, such as IPRs, working groups, teleconferences and technology exchange forums. Assist the Government in developing strategic plans, strategic assessments, and reviewing new capabilities.

C.4.14. Participate in integrated design teams, Operational Planning Team (OPT) and working groups to assist the Government in developing standardized process solutions, standards, and guidance.

C.4.15. Technical and Process Editing support functions: The Contractor shall:

C.4.15.1. Review all submitted documents for adherence to the guidance documentation, including the latest U.S. Government Printing Office Style Manual, AR 25-50, and NETCOM PAM 25-52.

C.4.15.2. Ensure documents have proper classification markings, in the correct format, contain proper capitalization, use of typefaces, numerals, compound words, spacing before and after dashes and symbols, and use of correct spelling and grammar. Table of contents agrees with heading in text, and page numbers are correct. Tables, figures, references, equations, and footnotes numbered and identified correctly, and references to other documents are accurate. Ensure the document has no incomprehensible statements, caused by missing material.

C.4.15.3. Validate sources referenced within the document and identify missing or misleading information in source documents to the technical leads.

C.4.15.4. Maintain an electronic repository of document control, tracking and staffing control, code, modifications, and trend analysis.

C.4.15.5. Track routing, signature approval process, and workflow of assigned documents to assist the Government in ensuring documents meet project schedule timelines.

C.4.15.6. Consult with authors regarding document content, readability and consistency.

C.4.15.7. Develop and provide a monthly workload report to the COR detailing matrix support, document count and functional areas of support.

C.5.0. QUALITY CONTROL / QUALITY ASSURANCE

C.5.1. Quality Control
The Contractor shall develop a quality control plan (QCP) and implement a quality control program to satisfy the specific requirements of this contract. Specific performance metrics appear in Attachment A, Performance Requirements Summary. The QCP shall initially identify potential high-risk problem areas throughout the life of the contract to incorporate identified problem areas in the QCP developing optimal problem resolution and providing necessary feedback to the Government. The Contractor shall provide the QCP to the KO and COR for approval no later than 30 calendar days after contract award. The Contractor shall update the QCP as required and provide copies to the KO and COR for approval.

C.5.2. Quality Assurance
The Government will monitor the Contractor's performance under this contract. The Government has the right to conduct inspections and performance evaluation at any time. If any aspect of the performance is not in conformance with the requirements of this contract, the Government has the right to issue to the Contractor a Contract Discrepancy Report (CDR). The Contractor shall explain in writing why performance was not in conformance with the requirements of the contract, how performance will be returned to conformance, and how recurrence of the problem will be prevented in the future. The Contractor shall complete and return the CDR to the KO and COR within five workdays after receipt of the CDR. The Contractor shall maintain copies of all inspection and evaluation reports.

C.6.0. TECHNICAL DELIVERABLES

The Contractor shall provide the following deliverables in the following formats: Word, PDF, EXEL, Power Point and Microsoft Project to the COR or and as identified by the COR. Any additional deliverables and due dates not specified below will be specified by the COR.

PWS Paragraph	Deliverable Title	Deliverable Date
C.3.16.	VTC Connection Standard	1 hour (VIP)/30 minute (non-VIP) prior to event
C.3.18.	Security Compliance Report	Weekly, as tasked

PWS Paragraph	Deliverable Title	Deliverable Date
C.3.18.	Service Design Package Update	As tasked
C.3.18.	System Continuity of Operations Plan Draft and Update	Ongoing, within 15 business days of tasking
C.3.19.	Enterprise System Project Plan Status Report	Weekly, as tasked
C.3.20.	Web Service and Business Intelligence Environment Performance Report	Weekly, as tasked

C.6.1. Product Compatability
The Contractor shall provide the product or a reproducible copy of the product on optical media in an automated format that is compatible with the Government office applications software. Applications currently being used by NETCOM are the Microsoft Office Suite, Windows 7, Windows 8, and Windows 10 operating systems. The Contractor shall comply with NETCOM Pamphlet 25-52 rules for grammar and usage when preparing all documentation.

C.7.0. ADMINISTRATIVE DELIVERABLES
These deliverables are administrative in nature and the Contractor shall not be required to obtain receipt and acceptance from the Government nor shall the Contractor be required to maintain these administrative deliverables in the archive provided for in paragraph C.7.5. The Contractor shall provide the following administrative deliverables. Any additional administrative deliverables and due dates not specified below and number of copies will be specified by the COR.

C.7.1. Meeting minutes of In-Progress Reviews (IPR), and technical meetings, as tasked, in Microsoft Word via email due no later than the end of the next business day.

C.7.2. Trip Reports, due no later than 3 working days after return.

C.7.3. Monthly Contractor Progress, Status and Management Report. The Contractor shall meet weekly with the COR to provide project status. The Contractor shall provide a soft and two hard copies of a comprehensive monthly status, progress and management report to the COR

C.7.4. Weekly Situational Report (SITREP) due by 1600hrs each Monday to the COR and the Government Task Monitor.

C.7.5. Electronic, indexed, archival record of all deliverables delivered under this contract shall be maintained by the Contractor. All administrative deliverables outlined in this PWS are exempt from the requirements of this provision. The archive shall be delivered to the COR upon request.

C.8.0. ADMINISTRATIVE REQUIREMENTS

C.8.1. Phase-In. The Contractor shall conduct phase-in procedures beginning 21 calendar days prior to the performance date. The phase-in shall require coordination with the incumbent Contractor.

C.8.2. Phase-Out. The services under this contract are considered vital to the Government and must be continued without interruption upon contract expiration. Therefore, the Contractor shall provide phase-out services IAW FAR 52.237-3.

C.8.3. Meeting with the Requiring Activity. The Contractor shall coordinate all meetings with the requiring activity in advance through the COR.

C.8.4. Place of Work and Work Hours – Currently for tasks at Ft. Huachuca, the Contraor's primary place of work is at NETCOM, Greely Hall, Ft. Huachuca, AZ 85613. Support for NETCOM sites in Korea, Hawaii, Ft. Bragg, Ft. Carson, Kuwait, Ft Belvoir, Ft Gordon, and other Post, Camps, Stations, may be designated primary work locations, as required, and approved by the KO through a contract modification. The Contractor shall be required to provide support at other NETCOM locations in a TDY status that will be identified by the GTL and approved by the COR, as required. Prior to any travel, the COR must approve work performed at locations other than Ft. Huachuca and the other locations defined above in advance. Primary work location shall be approved by the KO prior to work performance.

C.8.4.1. Work and place of duty locations during the first option year and subsequent years, the contractor shall provide labor support to RCC-P (Hawaii), RCC-K (Korea), and RCC-SWA (Kuwait), as required, per modification and exercising of the first option year.

C.8.4.2. ACCESS TO CLASSIFIED INFORMATION IS LIMITED TO GOVERNMENT WORK LOCATIONS. NO CLASSIFIED INFORMATION SHALL BE DISCUSSED, PROCESSED, OR STORED IN THE CONTRACTOR'S FACILITY.

C.8.4.3. Core work hours - The workday shall be consistent with the 24/7 work schedule provided to the government by the contractor. A regularly scheduled lunch break must be taken IAW the company's policy for lunch. The Contractor shall coordinate employees' proposed normal workday schedules with the COR to ensure they will meet mission requirements before the employees' start date.

C.8.4.2.2. Other Than Normal Duty Hour Call-back. The Contractor may be required to provide services outside the core hours (call-back), including holidays and weekends. The contractor shall provide a manning roster and on-call roster for emergency service support after duty hours. All terms and conditions of the contract apply during the performance of call-back hours.

C.8.4.2.3. The COR will either contact the Contractor for telephonic support or give the Contractor advance notification of at least one hour should contractor personnel need to report to the work site. Advance notification will be provided whenever possible. An exception to this may occur when emergencies arise, in which case advance notice may not be given. The COR will contact the Contractor in the event of an emergency. The Contractor shall respond to emergency calls and arrive at the designated work site within two hours after receiving the emergency call.

C.8.4.2.4. The contractor shall provide a manning roster and work schedule, by position, to the Government IAW the PWS requirements, monthly or when changes occur. The Contractor shall provide a leave and training schedule for personnel identified in the above-mentioned roster to the COR on a

monthly basis, in a soft copy, format to be specified by the COR, no later than two workdays prior to the month for which the schedule is applicable.

C.8.4.2.5. The Contractor will be paid for the actual time worked for telephonic support by the Government, or when called back to work for unscheduled time outside core hours on a day when the employee is normally scheduled for work. Irregular or occasional overtime work performed by the Contractor on a day when work was not scheduled, or for which the Contractor is required to return to place of employment is considered overtime and only actual hours worked are billable and subject to overtime pay.

C.8.5. Travel - The Contractor shall provide support at CONUS and OCONUS locations. The designated on-site support outside Ft. Huachuca, AZ (Support for GEF sites at Guam, Grafenwoehr, Ft. Bragg, Ft. Carson, Rock Island Arsenal, and Kuwait may be designated primary locations during Option Year 1, pending Government approval and workload determination) will be designated as TDY. The Contractor shall obtain all necessary travel documents to execute travel as required, including but not limited to U.S. Government-issued passports to support OCONUS travel requirements. The Contractor shall ensure all Contractor employees comply with all guidance, instructions, and general orders applicable to U.S. Armed Forces and DoD civilians and issued by the Theater Commander or his/her representative. This shall include any and all guidance and instructions issued based on the need to ensure mission accomplishment, force protection, and safety. The Government will reimburse the Contractor, in accordance with the Joint Travel Regulation (JTR) and FAR part 31.205-46, for all approved travel incurred during the performance of this contract. The COR will approve all travel requirements before travel begins.

C.8.5.1. The COR will issue travel subtasks via email to the Contractor that include destination, dates, duration of stay, purpose, and estimated cost. Travel requests for deployment will specify additional travel conditions. The Contractor shall not proceed without this notification and adequate contract funding.

C.8.5.1.1. Travel to other OCONUS Locations. The Contractor may be required to travel to various OCONUS locations, such as Southwest Asia (SWA), and may be required to perform under extreme conditions. The Government will provide the Contractor a Letter of Authorization (LOA) for billeting, meals, and other amenities as required. The Government and the Contractor will fulfill all current regulatory and policy requirements before travel, such as; ISOPREP, area specific training, immunizations, etc.

C.8.5.1.2. The Contractor shall coordinate all contractor travel requirements with appropriate Government personnel within NETCOM at each location in advance of the actual travel to minimize the impact on Government travel requirements.

C.8.5.1.3. Synchronized Predeployment Operational Tracker (SPOT): The prime Contractor shall enter before deployment and maintain data for all Contractor personnel to include sub-contractors that are authorized to accompany U.S. Armed Forces deployed outside the United States as specified in paragraph (b)(1) of this clause. The Contractor shall use the Synchronized Predeployment and Operational Tracker (SPOT) web-based system, at https://spot.dmdc.mil/privacy.aspx, to enter and maintain the data.

C.8.5.1.4. The prime Contractor is responsible to close out the deployment of personnel, including subcontractor employees at all tiers, at the end of the contract completion period and to release the personnel from the prime Contractor's company in the SPOT database IAW DFARS 252.225-7040 or DFARS DOD class deviation 2011-O0004 this class deviation is now archived, is there a new one?. The release of employee information must be accomplished no more than 30 calendar days after the end of the contract/task order completion date.

C.8.5.1.5. Accountability of Prime and Subcontractor Personnel: Whether specifically written into the contract or not, it is the expectation of the Government that for any persons brought into the theater of operation for the sole purposes of performing work on Government contracts, contract employers will return employees to their point of origin/home country once the contract is completed or their employment is terminated for any reason. If the prime Contractor fails to re-deploy an employee, or subcontractor employee at any tier, the Government shall notify the applicable U.S. Embassy to take appropriate action. Failure by the prime Contractor to re-deploy its personnel, including subcontractor personnel at any tier, at the end of the contract completion date, could result in the contractor being placed on the Excluded Parties List System (EPLS) and not be allowed to propose on future U.S. contracts anywhere in the world.

C.8.5.2. Travel to Germany.

C.8.5.2.1. Contractors traveling to Germany for TDY shall use the Technical Expert Status Accreditation/Analytical Support Accreditation (TESA/ASSA) TDY procedures. The complete instructions are available at the DoD Contractor Personnel Office (DOCPER) website at http://www.eur.army.mil/g1/content/CPD/docper/docper_germanyLinks.html?tab=5&framepage=tesa.html. Under the Technical TESA/ASSA TDY procedure, contractors would be entitled to logistical support and applicable tax exemptions.

C.8.5.2.2. Before the Contractor begins work in Germany, the COR for the Contractor seeking TE accreditation under this procedure will complete the TESA/ASSA TDY Application online through the DOCPER Contractor Online Processing System (DCOPS) and submit it, along with required uploaded documents, to DOCPER. The application form (AE 715-9D) must be printed from DCOPS, signed by the COR and the applicant, and then be scanned and uploaded into DCOPS.

C.8.5.2.3. Applications submitted to DOCPER more than 90 days in advance of the arrival date will be returned without action. [Note: The time between approval of the DD 1172-2 by DOCPER and the issuance by the ID card facility must be less than 90 days.] If the individual is determined to be qualified and is performing work in an approved position on an approved contract, DOCPER will approve technical expert status (and an ID card) for a limited period of time (not to exceed 90 days). [Note: Because ID card facilities will not issue ID cards for periods less than 30 days, 1172-2s issued by DOCPER will reflect a minimum of 30 days.]

C.8.5.2.4. Each period of TESA/ASSA TDY requires a separate TESA/ASSA TDY application. TESA/ASSA TDY is limited to a cumulative total of 90 days or three approved requests, whichever occurs first, within a 12-month period. The latter restriction concerning the number of approved requests is a function of the 30-day minimum approval period as three requests for short periods of TESA/ASSA TDY over a period of time still equate to the maximum of 90 days.

C.8.5.3. Travel to Republic of Korea (ROK).

C.8.5.3.1. U.S. Government contractors who travel to ROK must be identified as Invited Contractors/Technical Representatives (IC/TR). Reference is United States Forces Korea (USFK) Regulation 700-19 (The Invited Contractors and Technical Representatives Program).

C.8.5.3.2. The COR will inform the KO of any anticipated contractor travel to Korea as soon as the requirement is known. The COR will ensure that the Sponsoring Agency (SA) has been identified, and that the SA has appointed a Responsible Officer (RO). The RO shall ensure the completed USFK Form 700-19A-R-E and Letter of Accreditation (LOA) are submitted USFK/FKAQ no later than 30 calendar days prior to travel. USFK/FAQ will review, process, stamp, and complete Part III of the USFK Form 700-19A-R-E.

C.8.5.3.3. Status of Forces Agreement (SOFA) ensures that SOFA provisions on legal and jurisdictional issues and official support mechanisms are applied to the Contractor while on official business. In order to obtain SOFA status in Korea, the Contractor employees shall present a DOD identification card obtained stateside prior to travel, passport with A-3 Visa, LOA, red-stamped USFK Form 700-19A-R-E, and copies of each document to Korean immigration authorities.

C.8.5.3.4. Training Requirements for IC/TR personnel shall be conducted in accordance with USFK Reg 350-2 Theater Specific Required Training for all Arriving Personnel and Units Assigned to, Rotating to, or in Temporary Duty Status to USFK. IC/TR personnel shall comply with requirements of USFK Reg 350-2. The COR will provide necessary instructions for accessing and completing this training.

C.8.6. SECURITY REQUIREMENTS. 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 the Security Agreement (DD Form 441), including the National Industrial Security Program Operating Manual (DoD 5220.22-M) and any revisions to DoD 5220.22-M.

C.8.6.1. Contractors will require access to classified facilities. Highest level security clearance requirement for this work effort is Secret. Upon contract performance start date, all Contractor personnel shall, possess a SECRET security clearance.

C.8.6.2. Contractor personnel who require a Secret security clearance and who will require IT Level I system access or who will be performing IT level I functions require a Tier 5 (T5) investigation completed with a favorable fitness determination for IT Level I access. If Contractor personnel do not have a favorable T5/T5 Reinvestigation (T5R) on record, the Contractor shall contact the supporting Government Security Office/G2/S2 for submission of the T5 investigation (SF 86). The Contractor shall provide the contract number as authority to request the investigation. Contractor interim privileged level access to Army systems prior to, completion with a favorable fitness determination of the required investigation, will be in accordance with AR 25-2.

C.8.6.3. All contractor personnel who require access to classified COMSEC information shall have a FINAL security clearance at the requisite level and will be subject to the Department of the Army Cryptographic Access Program (DACAP) if access meets the criteria in AR 380-40, Chapter 7. See DD Form 254, Contract Security Classification Specification for additional information and requirements.

C.8.6.4. All Contractor personnel shall have the required security clearance at contract performance start date and shall maintain the required security clearance over the life of the contract, in accordance

with the DD Form 254, Contract Security Classification Specification. New or replacement personnel shall have the required security clearance at work performance start date. Cleared Contractor personnel may require access to SIPRNET or other classified systems in support of this work effort. Access to classified systems will only be at specified Government work locations and will be sponsored by the COR.

C.8.6.5. Threat Awareness and Reporting Program (TARP) Training. All contractor personnel assigned to this contract shall complete initial and annual TARP training. Completion of training shall be reported to the COR. Detailed requirements on TARP are stated in the DD Form 254, Contract Security Classification Specification.

C.8.6.6. Contractor personnel shall comply with all applicable security regulations, guidance, and procedures referenced in the PWS, the DD Form 254, and in effect at the Government work sites. This includes regulations and procedures for entry to the installation and entry to restricted/controlled areas and facilities.

C.8.6.7. Access and General Protection Security Policy and Procedures. Contractor and all associated sub-contractor employees shall provide all information required for background checks to meet installation access requirements to be accomplished by the installation Provost Marshal Office (PMO), Director of Emergency Services (DES), or Security Office. Contractor workforce shall comply with all personal identity verification requirements of FAR clause 52.204-9, Personal Identity Verification of Contractor Personnel. In addition to the changes otherwise authorized by the changes clause of this contract/task order, should the Force Protection Condition (FPCON) at any individual facility or installation change, the Government may require changes in contractor security matters or processes.

C.8.6.8. Security In/out processing. All Contractor personnel integrated or embedded with NETCOM organizations shall in-process through the supporting NETCOM organizational G-2 Security Office at work performance start date. All Contractor personnel integrated or embedded with NETCOM organizations shall out-process and clear through the supporting NETCOM organizational G-2 Security Office upon termination of employment on the contract or upon contract expiration/termination, whichever occurs first. Above requirements are applicable if there is a change in primary work performance location while employed on the contract. The prime Contractor shall ensure above requirements are included in sub-contracts and lower tier contracts when personnel are integrated or embedded with NETCOM organizations. Per AR 380-49, “embedded and/or integrated contractors are those who operate out of government-supplied on-base space.”

C.8.7. Protection

C.8.7.1. Cybersecurity - Information Assurance

C.8.7.1.1. Information Assurance (IA) Training. All Contractor personnel with access to Government information systems and networks shall successfully complete all required initial and annual IA awareness training as specified in AR 25-2 and as specified by the Government requiring activity. Training is available at https://ia.signal.army.mil.

C.8.7.1.2. Contractor employees and subcontractor employees performing work under this contract who have access to Government information systems and networks shall create a user account and profile in the Army Training and Certification Tracking System (ATCTS) located at https://atc.us.army.mil, in the

unit container designated by the COR. Certificates of successful completion of IA training, Acceptable Use Policies (AUP), applicable baseline and computing environment (CE) certifications, and continuing professional education credits, as required by DoD 8570.01-M, shall be uploaded to the ATCTS and provided to the COR for continuous compliance monitoring and reporting.

C.8.7.1.3. The Contractor shall ensure that all Contractor employees and subcontractor employees requiring IA awareness training complete the training at the start of work performance on this contract and annually thereafter for the duration of this contract.

C.8.7.2. Information Assurance Workforce Certification. DFARS clause 252.239-7001 (Information Assurance Contractor Training and Certification) applies to this contract. This contract is subject to the mandates of DoD 8570.01-M, which establishes baseline technical and management IA skills for personnel performing IA functions within DoD. Functions spanning multiple levels require certification of the highest level functions. Contractor personnel performing functions in multiple categories or specialties shall hold certifications appropriate to the functions performed in each category or specialty.

C.8.7.2.1. The Contractor shall ensure its IA workforce members have the baseline certifications corresponding to their IA functions, as defined in Chapters 3, 4, 5, 10, and 11, and Appendix 3 of DoD 8570.01-M at work performance start date. Contractors will obtain all required Computing Environment (CE) certificates within 6 months of being engaged. The IAT Level I baseline certification is the minimum requirement for unsupervised privileged access. The Contractor shall ensure that all employee certifications remain active and are renewed prior to expiration.

C.8.7.2.2. The Contractor shall ensure that all employees IA certifications are released to the Department of Defense through the Defense Workforce Certification Application at https://www.dmdc.osd.mil/milconnect.

C.8.7.2.3. Table 1 reflects the Personnel Security (IT Level) and IA Workforce Specialty requirements, aligning the IA functional responsibilities and access levels to the contract, in accordance with DoD 8570.01-M.

Table 1. Information Technology Access and IA Certification Requirements.

Functional Area	IT Level (IAW AR 25-2)	Security Clearance	Investigation Required	IA Certification Category and Level (IAW DoD 8570.01-M and BBP 05-PR-M-0002)	Computing Environment Certifications
Help Desk Support Service Specialist	II	SECRET	Tier 3	IAT-II	Yes
Software Engineer	I	SECRET	T5	IAT-II	Yes

Systems Administrator	I	SECRET	T5	IAT-II	Yes
Network Administrator	I	SECRET	T5	IAT-II	Yes
Senior IT Systems Solution Architect	II	SECRET	T3	IAT-III	Yes
Systems Engineer	I	SECRET	T5	IAT-II	Yes
Audio Visual Programmer	II	SECRET	T3	IAT-II	Yes

C.8.7.3. Non-Government-owned computing systems or devices. The Contractor shall comply with AR 25-1 and AR 25-2. The Contractor shall not install or connect non-Government-owned computing systems or devices to Government networks without the COR's coordinating and obtaining proper authorization from the appropriate Information Systems Security Manager (ISSM), ensuring that all software has a Government Certificate of Networthiness or has been authorized under the Risk Management Framework (RMF) Assess Only process. The non-Government-owned computing systems or devices include, but are not limited to, personal or Contractor-owned thumb drives (e.g., memory sticks, flash drives, Universal Serial Bus (USB) drives, jump drives, pen drives), removable or external hard drives, Personal Digital Assistants (PDA), PC Cards/Express Cards, MP3 players, cell phones, digital media, floppy disks, compact disc (CD)/digital video disk (DVD) burners, optical recordings, photo flash cards, laptops, or any devices that can store data.

C.8.7.3.1. In the event the Contractor is required to work at off-site facilities, only Government Property shall be used to access the VPN. Per AR 25-1, paragraph 4-1e, the only authorized access from DoD-owned computers, systems, and networks to the Internet is via the NIPRNet. The VPN allows remote DoD computers to meet this requirement by providing a secure tunnel to the NIPRNet. The VPN must be used at all times that the DoD-owned computer is accessing the Internet when using commercial Internet Service Providers.

C.8.7.3.2. No Contractor or Employee-Owned Information Systems (EOIS) are allowed connection or access via the VPN. The NIPRNet is Sensitive Information. AR 25-2, paragraph 4-31a, prohibits the use of EOIS for sensitive information. Non-Army Government agencies will require evaluation on case-by-case basis. Non-DoD hosts will be treated as un-trusted hosts.

C.8.7.4. Protection of Sensitive Unclassified Data. The Contractor shall ensure any sensitive information, including, but not limited to, Personally Identifiable Information (PII) and For Official Use Only (FOUO), proprietary, and Law Enforcement Sensitive information residing on Mobile Computing Devices (MCD) or other external media, is protected in accordance with current Data at Rest (DAR) guidelines and requirements. The Contractor shall use an authorized, approved, and prescribed DAR solution. The MCDs include, but are not limited to, laptop, netbook, notebook, or tablet computers, and Blackberry or equivalent devices. External media include optical disk media such as CDs, DVDs, USB drives (also referred to as flash or thumb drives) (when authorization to use them is restored), floppy disks, and other portable digital storage devices.

C.8.8. Antiterrorism.

C.8.8.1 Antiterrorism Level I Training. The Contractor shall ensure that all contractor employees, including subcontractor employees, requiring access to Army installations, facilities, or controlled access areas complete Antiterrorism (AT) Level I awareness training within 30 calendar days after start of employee performance on this contract. Within 5 calendar days after successful completion of training, the Contractor shall certify to the COR or KO that all employees performing work under this contract have completed the AT Level I awareness training. AT Level I awareness training is available at https://jkodirect.jten.mil, course # - US007. This training is in addition to any required unit or theater specific AT Level I training which may be more stringent based on area of operation or need for heightened awareness.

C.8.8.2. Outside Continental United States (OCONUS) Travel. If this contract requires OCONUS travel, Contractor employees shall obtain KO or COR approval prior to such travel. The Contractor employees shall contact the Government requiring activity Antiterrorism Office (ATO) to receive a specific theater AT/threat briefing prior to departing on OCONUS temporary duty travel and complete IOSPREP training. Contractor shall provide the ISOPREP certificate to the COR with all OCONUS travel requests.

C.8.8.3. iWATCH. The Contractor shall ensure that all employees and subcontractor employees performing work under this contract are trained on the local iWATCH program within 30 calendar days of start of employee performance on this contract. The requiring activity ATO will provide the locally developed iWATCH training. The Contractor shall maintain all iWATCH training records and shall provide copies to the COR upon request.

C.8.8.4. Emergencies and Force Protection Conditions. During declared emergencies and/or elevated Force Protection Conditions (FPCONs) Charlie or Delta, contractor performance under this contract shall be determined by the COR or KO. All Contractor employees providing services under this contract are required to report for duty as scheduled and remain on duty during declared emergencies and/or elevated FPCON levels unless otherwise directed by the KO or COR. The Contractor Project Manager shall keep the COR apprised of all personnel whereabouts (e.g. dates, location) when in a temporary duty (TDY) status.

C.8.9. Operations Security (OPSEC). The Contractor shall comply with DoD Directive 5205.02E, Army Regulation 530-1, and the requiring activity OPSEC program. The Contractor shall ensure all contractor employees and subcontractors performing work under this contract complete Level I OPSEC training within 30 calendar days of start of employee performance on this contract and annually thereafter. The Contractor shall maintain all OPSEC training records and shall provide copies to the COR upon request. Annual refresher training shall be completed on-line at: http://cdsetrain.dtic.mil/opsec/. A record of completion will be provided to the COR and unit/activity security manager. (Ref AR 530-1.)

C.8.10. Contractor Identification Requirements. In accordance with FAR 37.114 (c), all Contractor personnel attending meetings, answering Government telephones, and working in other situations where their contractor status is not obvious are required to identify themselves as such to avoid being mistaken for Government officials. Contractors performing work at Government workplaces shall provide their employees with an easily readable identification (ID) badge indicating the employee's name, the contractor's name, the functional area of assignment, and a recent color photograph of the employee. Contractors shall require their employees to wear the ID badges visibly when performing work at Government workplaces. Contractor personnel shall also ensure that all e-mails, documents or

reports they produce are suitably marked as Contractor products and/or that Contractor participation is appropriately disclosed. All signature blocks on e-mails shall indicate that the sender is a Contractor employee and include the Contractor's company name.

C.8.11. Common Access Card (CAC). The Government will provide special access badges as necessary. The Prime Contractor Facility Security Officer (FSO) shall ensure that all Contractor personnel acquire and maintain CACs. The approving Government Trusted Agent (TA) may give access to the FSO using the online Trusted Associate Sponsorship System (TASS), https://www.dmdc.osd.mil/tass. Contractor eligibility remains in force during employment under the contract for those employees who have a valid and recurring requirement for access to Government facilities or automation systems (reference DD254 for additional security requirements) to perform those duties stipulated in the contract. The Contractor shall use a valid CAC to access the Government domain. The Contractor shall immediately return the CACs to the COR when the Contractor employee's employment is terminated or upon expiration of the contract. The CACs will expire when Contractor employee's eligibility terminates or three years from the issuance date, whichever occurs first. The Contractor is responsible for all CACs and shall report all lost or stolen CACs to the COR immediately.

C.8.12. Access to Protected Information. Protected information means all non-public information, including, but not limited to, trade secrets or proprietary information of other Contractors, Government source selection information, Privacy Act or personally identifiable information (PII), or any other information with distribution limited by the Government. If, during the performance of this requirement, Contractor personnel obtain access by any means to protected information, they shall not disclose, publish, divulge, release, or make known, in any manner or to any extent, the information except as necessary to carry out duties under this contract. Protected information shall be given only to persons specifically granted access to this sensitive information and may not be further divulged without specific prior written approval from an authorized U.S. Government individual. Further, contractor employees may use any non-public information for official/authorized Government purposes, and they shall not use the information for their personal gain, the gain of their employer, or the gain of anyone else. The Contractor shall notify the KO of any potential organizational conflicts of interest created by any such access; however, a nondisclosure agreement will not overcome an Organizational Conflict of Interest (OCI) as defined in FAR Subpart 9.5. Moreover, the Trade Secrets Act prohibits releasing proprietary information without the owner's consent. Accordingly, all Government Contractors are required to mark their proprietary information, and any time the Contractor is given inadvertent access to such marked information, the Contractor shall inform the KO of the access.

C.8.13. Accounting For Contractor Support. The Office of the Assistant Secretary of the Army (Manpower & Reserve Affairs) operates and maintains a secure Army data collection site where the Contractor shall report ALL Contractor manpower (including sub-contractor manpower) required for performance of this contract. The Contractor is required to completely fill in all the information in the format using the following web address https://cmra.army.mil. Wrong address for CMRA reporting, should be using this site: https://armycmra.dmdc.osd.mil The required information includes: (1) Contracting Office, Contracting Officer, Contracting Officer's (Technical) Representative; (2) Contract number, including task or delivery order number; (3) Beginning and ending dates covered by reporting period; (4) Contractor name, address, phone number, e-mail address, identity of Contractor employee entering data; (5) Estimated direct labor hours (including sub-contractors; (6) Estimated direct labor dollars paid this reporting period (including sub-contractors); (7) Total payments (including sub-contractors); (8) Predominant Federal Service Code (FSC) reflecting services provided by Contractor (and separate predominant FSC for each sub-contractor if different); (9) Estimated data collection cost; (10)

Organizational title associated with the Unit Identification Code (UIC) for the Army Requiring Activity (the Army Requiring Activity is responsible for providing the Contractor with its UIC for the purposes of reporting this information); (11) Locations where the Contractor and sub-contractors perform the work (specified by zip code in the United States and nearest city, country, when in an overseas location, using standardized nomenclature provided on website); (12) Presence of deployment or contingency contract language; and (13) Number of Contractor and sub-contractor employees deployed in theater this reporting period (by country). As part of its submission, the Contractor shall also provide the estimated total cost (if any) incurred to comply with this reporting requirement. Reporting period will be the period of performance not to exceed 12 months ending September 30 of each Government fiscal year and must be reported by October 31 of each calendar year. Contractors may use a direct XML data transfer to the database server or fill in the fields on the website. The XML direct transfer is a format for transferring files from a Contractor's systems to the secure web site without the need for separate data entries for each required data element at the web site. The specific formats for the XML direct transfer may be downloaded from the web site. The Contractor shall report ALL contractor labor hours (including subcontractor labor hours) required for performance of services provided under this contract for the Army via the eCMRA secure data collection site. The contractor is required to completely fill-in all required data fields within the eCMRA. Reporting inputs will be for the labor executed during the period of performance during each Government fiscal year (FY), which runs October 1 through September 30. While inputs may be reported any time during the FY, all data shall be reported no later than October 31 of each calendar year. Contractors may direct questions to the help desk at: http://www.ecmra.mil/.

C.8.14. The Civilian Tracking System Reporting Requirement - The Department of the Army has a requirement to record the movement of deployed employees/civilians. The Army Contractor Personnel Account requires the civilian tracking system to maintain accountability for Contractor employees and Civil Service employees deployed outside continental United States in an operational Theater. The Contractor is required to input deployed civilian information on a daily basis. The Web site is https://cpolrhp.belvoir.army.mil/civtracks/default.asp- could not open this site.

C.8.15. Safety. The Contractor shall perform in a manner that assures maximum safety and protection for their employees and all personnel while performing work for this contract. The Contractor shall exercise surveillance on a continuing basis and shall eliminate or otherwise control existing or potential safety hazards.

C.8.15.1. The Contractor shall participate in the Government's safety program. Compliance with provisions pertaining to safety of site facilities and equipment is mandatory. The Contractor shall establish and implement a comprehensive Safety Program Plan for use by contractor and sub-contractor employees. This Plan shall incorporate appropriate elements of 29 CFR 1910 and 1926, AR 385-10, NETCOM Reg 385-1 and applicable OSHA regulatory guidance. The Contractor shall provide the COR and KO with its Safety Program Plan within 30 calendar days of contract award for acceptance. The COR and KO will approve all updates to the Safety Program Plan before implementation.

C.8.15.2. The Contractor shall comply with all federal, state and local policies, directives, laws and regulations. During the performance of tasks requiring protective equipment and clothing, contractor employees shall wear safety items required by OSHA and as specified in the applicable regulations. The Contractor shall be responsible for providing personal protective equipment, clothing and training.

C.8.15.3. The COR may require the Contractor to cease operations associated with the performance of this contract for safety violation reasons. The Contractor shall correct any safety violations, caused by a contractor employee, during non-duty hours at no additional cost to the Government.

C.8.15.4. The Contractor shall ensure all employees receive the safety training required by all federal, state and local laws and policies. The Contractor shall maintain the safety training records and make them available to the COR and KO upon request.

C.8.16. Key Personnel - The Contractor shall assign and identify a site lead who will be considered key to operations under this contract. The site lead shall provide management, administrative, and technical interface with Government personnel in the day-to-day accomplishment of support services. This individual must have an in-depth understanding of the requirements and their responsibilities, and the ability, knowledge, experience, and skills to perform the requirements.

C.8.17. Specialized Training for Contractor Personnel.

C.8.17.1. The Contractor shall provide technically proficient personnel capable of performing the contract requirements. The Contractor shall have processes and procedures to provide required initial, refresher, upgrade and proficiency training for personnel in order to maintain pace with technological advances to perform the contract requirements at no additional cost to the Government. The Government shall provide training to meet special requirements of a particular task within the PWS, such as with a new or unique software application or new equipment or systems. Sustainment or follow-on training may be obtained from the original equipment manufacturer and will be at the Contractor's expense. The COR shall authorize the training in advance. If an employee who has received Government-provided training leaves the contract, the Contractor shall provide certified, trained and properly cleared replacement personnel at no additional cost to the Government. The Contractor shall maintain training documentation and certifications for all employees and make them available to the COR upon request.

C.8.17.2. The Contractor shall have processes and procedures in place to provide required supplemental, refresher, upgrade, and proficiency training for personnel in order to maintain pace with technological advances at no additional cost to the Government. The Government may provide additional training at its discretion.

C.9.0 GOVERNMENT PROPERTY

C9.1 There will be no Government Furnished Property (GFP) under this contract. In accordance with FAR Part 45.00 (5) the Government will provide Government property that is incidental to the place of performance.

C.9.2 Incidental Property. The Government will provide property incidental to the place of performance, when the contract requires contractor personnel to be located on a Government site or installation, and when the property used by the contractor within the location remains accountable to the Government. Items considered to be incidental to the place of performance include normal office type property, for example, office space, desks, chairs, telephones, computers, printers, plotters, fax machines and computer peripherals. It does not include any equipment, special test equipment, special tooling, material or real property.

C.9.3 Contractor Property. The Contractor shall provide all equipment, and items required to perform the requirements of this contract unless provided as incidental as indicated above or listed. All Contractor provided equipment shall be clearly marked and stored separately from Government property. Upon completion or termination of this contract, the Contractor shall remove all Contractor-owned equipment/property. If the Contractor does not remove Contractor-owned items NLT thirty (30) calendar days after the conclusion of the contract, the Government will properly dispose of the items.

C.10.0. GOVERNMENT POINTS OF CONTACT (POC)

The COR will be the primary Government POC for this contract. The KO will provide the Contractor a copy of the COR Designation Letter for this contract upon award. The Contractor shall acknowledge the COR Designation Letter in writing and return to the KO within 5 business days of receipt. Other Government POCs will be identified as required.

C.11.0. APPLICABLE DOCUMENTS

The following publications form a part of this contract. The publications below with which the Contractor shall comply are "Mandatory." The Contractor shall use current commercial practices and publications whenever possible. A significant number of Army regulations that govern the conduct of the required work are listed below. The PWS may set a higher standard of performance than an applicable Army regulation. The PWS will have precedence over the regulations unless a particular PWS provision is in direct conflict with the applicable provision of the Army regulation. Unless otherwise noted, the publications can be accessed at www.apd.army.mil. Upon request, the Government will provide those publications not available on a web site. The Contractor shall comply with changes to publications. The Contractor shall inform the KO of any changes to a publication or documents that impact the cost of the contract/task order. Additional technical design and policy reference information governing the SIPRNet can be accessed at http://iase.disa.mil/policy-guidance/index.html#trustedproducts and http://iase.disa.mil/stigs/iadocs.html.

AR 25-1	Army Information Technology
AR 25-2	Information Assurance
AR 25-50	Preparing and Managing Correspondence
AR 25-55	Department of the Army Freedom of Information Act Program
AR 190-13	The Army Physical Security Program (FOUO requires AKO access)
AR 190-51	Security of Unclassified Army Property (Sensitive and Non-sensitive)
AR 350-1	Army Training and Leader Development
AR 380-5	Department of the Army Information Security Program
AR 380-40	Policy for Safeguarding and Controlling Communications Security (COMSEC) Material (FOUO, requires AKO access)

AR 380-49	Industrial Security Program
AR 380-67	Personnel Security Program
AR 381-12	Threat Awareness and Reporting Program (TARP)
AR 385-10	The Army Safety Program
AR 525-13	Antiterrorism (FOUO)
AR 530-1	Operations Security (OPSEC)
DA Pam 25-1-1	Army Information Technology Implementation Instructions
DCID 6/6	Security Controls on the Dissemination of Intelligence Information
DoD 5220.22-M	National Industrial Security Program Operating Manual (NISPOM)
DoD 8570.01-M	Information Assurance Workforce Improvement Program
DoDD 5205.02E	DoD Operations Security (OPSEC) Program
DoDD 5400.11	DoD Privacy Program
DoDD 8140.01	Cyberspace Workforce Management
DoDI 8500.01	Cybersecurity
DoDI 8510.01	Risk Management Framework (RMF) for DoD Information Technology (IT)
DoDM 5200.01-V1	DoD Information Security Program: Overview, Classification, and Declassification
DoDM 5200.01-V2	DoD Information Security Program: Marking of Classified Information
DoDM 5200.01-V3	DoD Information Security Program: Protection of Classified Information
DoDM 5200.01-V4	DoD Information Security Program: Controlled Unclassified Information (CUI)
JTR	Joint Travel Regulation
TB 380-41	Security: Procedures for Safeguarding, Accounting and Supply Control of COMSEC Material (FOUO)
NETCOM Regulation 25-56	Personally Identifiable Information
NETCOM Regulation 25-70	Web Content Administration, Policies, and Procedures

NETCOM Regulation 380-5 Information Security

NETCOM Regulation 385-1 Safety and Occupational Health

NETCOM Pamphlet 25-52 Writing, Grammar, and Style

NETCOM TTP Assess and Authorize v2.1

NETCOM TTP Bid Tracker v1.4

NETCOM TTP Organizational Policy Records v1.0

NETCOM TTP Security Control Assessor – Representative v1.1

NETCOM TTP Security Control Assessor – Validator v2.0

NETCOM TTP Stand-Alone Information System and Close Restricted Network Assessment and Authorization v1.0

https://www.dmdc.osd.mil/milconnect/

https://rmfks.osd.mil/rmf/Pages/default.aspx

Army CIO/G-6 Best Business Practice 05-PR-M-0002, Information Assurance (IA Training and Certification) available at https://www.milsuite.mil/wiki/)

U.S. Government Printing Office Style Manual (available at http://www.gpo.gov/fdsys/pkg/GPO-STYLEMANUAL-2008/pdf/GPO-STYLEMANUAL-2008.pdf)

Committee on National Security Systems Instructions (CNSSI) 4009, National Information Assurance Glossary (available at https://www.cnss.gov/CNSS/issuances/Instructions.cfm)

Memorandum, Department of the Army G-2, 29 May 2007, subject: Classified Visit Request Process

Memorandum, Office of the Under Secretary of Defense, 1 April 2005, subject: Facilitating Classified Visits within Department of Defense (available from the Government requiring agency)

Memorandum, Office of the Under Secretary of Defense, 5 December 2001, subject: Facilitating Necessary Access to NATO Classified Information (available from the Government requiring agency)

Operation Order (OPORD) 0910-300, 9th Signal Command (Army), 14 AUG 09, DAR Deployment

US Army Cyber Command and Second Army Security Classification Guide for Cyberspace Operations and Security, 19 May 2016 (FOUO available from the Government requiring activity).

XML Certification Program – XML Master available at www.XMLmaster.org/en/certifications.html#basic

C.12.0. DEFINITIONS AND ACRONYMS:

C.12.1. DEFINITIONS:

C.12.1.1. CONTRACTOR. A supplier or vendor awarded a contract to provide specific supplies or services to the Government. The term used in this contract always refers to the prime contractor.

C.12.1.2. CONTRACTING OFFICER (KO). A KO is a person with authority to enter into, administer, or terminate contracts and make related determinations and findings on behalf of the Government. The KO is the only individual who can legally bind the Government.

C.12.1.3. CONTRACTING OFFICER'S REPRESENTATIVE (COR). The COR is an employee of the U.S. Government appointed by the KO to administer the contract. This individual has authority to provide technical direction to the contractor as long as that direction is within the scope of the contract, does not constitute a change, and has no funding implications. This individual does NOT have authority to change the terms and conditions of the contract.

C.12.1.4. DEFECTIVE SERVICE. A service output that does not meet the standard of performance associated with the PWS.

C.12.1.5. DELIVERABLE. Deliverables are anything that can be physically delivered, but may include non-manufactured things such as meeting minutes or reports.

C.12.1.6. DIAGRAM. A plan, sketch, drawing, or outline designed to demonstrate or explain how something works or to clarify the relationship between the parts of a whole.

C.12.1.7. EXECUTIVE SUMMARY (EXSUM). Short document or section of a document, produced for business purposes, that summarizes a longer report or proposal or a group of related reports in such a way that readers can rapidly become acquainted with a large body of material without having to read it all. It will usually contain a brief statement of the problem or proposal covered in the major document(s), background information, concise analysis and main conclusions. It is intended as an aid to decision making by managers and must be short and to the point.

C.12.1.8. IDENTITY and ACCESS MANAGEMENT (IdAM). IdAM is the combination of technical systems, policies and processes that create, define, and govern the utilization, and safeguarding of identity information, as well as managing the relationship between an entity, and the resources to which access is needed. It can be divided into three fundamental capabilities: Manage Digital Identities, Authenticate Users, and Authorize Access to Resources.

C.12.1.9. INFORMATION TECHNOLOGY INFRASTRUCTURE LIBRARY (ITIL). IITIL is a set of practices for IT service management (ITSM) that focuses on aligning IT services with the needs of business.

C.12.1.10. KEY PERSONNEL. These are Contractor personnel that are considered to be essential to the work being performed under this contract.

C.12.1.11. PHYSICAL SECURITY. Physical security prevents the loss or damage of Government property.

C.12.1.12. QUALITY ASSURANCE SURVEILLANCE PLAN (QASP). The QASP is an organized, written document specifying the Government's surveillance methodology to be used for surveillance of contractor performance.

C.12.1.13. QUALITY CONTROL (QC). QC is all necessary measures taken by the Contractor to assure that the quality of an end product or service meets the contract requirements.

C.12.1.14. REMEDY/INFORMATION TECHNOLOGY SERVICE MANAGEMENT (ITSM). The implementation and management of quality IT services.

C.12.1.15. SUBCONTRACTOR. A person or company that enters into a contract with a prime contractor.

C.12.1.16. USER GUIDE. A user guide or user's guide is a technical communication document intended to give assistance to people using a particular system.

C.12.1.17. WHITE PAPERS. A report or guide helping readers to understand an issue, solve a problem, or make a decision

C.12.1.18. WORK DAY. The number of hours per day the Contractor provides services in accordance with the contract.

C.12.1.19. WORK WEEK. Monday through Friday, unless specified otherwise, by the COR.

C.12.2. ACRONYMS

ACofS	Assistant Chief of Staff
ACAS	Assured Compliance Assessment Solution
ACOIC	Army Cyberspace Operations and Integration Center
AEI	Army Enterprise Infostructure
AIES	Army Investigative Enterprise Solution
AKO	Army Knowledge Online
AO	Authorizing Official
API	Application Programming Interface
APMS	Army Portfolio Management Solution
AR	Army Regulation
ARCYBER	U.S. Army Cyber Command
ATCTS	Army Training and Certification Tracking System
ATO	Authority to Operate
AUP	Acceptable Use Policy
BCA	Business Cost Analysis
C4IM	Command, Control, Communications, Computers and Information Management
CA	Certifying Authority
CAC	Common Access Card
CAP	Certified Authorization Professional
CCB	Change Control Board
CCRM	Change Configuration Release and Management
ChM	Change Management
CISM	Certified Information Security Manager

CISSP	Certified Information Systems Security Professional
CM	Configuration Management
CONOPS	Concept of Operations
CONUS	Continental United States (excludes Alaska and Hawaii)
COOP	Continuity of Operation Plan
COR	Contracting Officer's Representative
CSD	Cybersecurity Directorate
DA	Department of the Army
DCO	Defensive Cyber Operations
DFARS	Defense Federal Acquisition Regulation Supplement
DISA	Defense Information System Agency
DMDC	Defense Manpower Data Center
DoD	Department of Defense
DoDIN	Department of Defense Information Network
ECS	Enterprise Collaboration Services
ELA	Enterprise License Agreement
eMASS	Enterprise Mission Assurance Support Service
EOIS	Employee-Owned Information Systems
ETP	Enterprise Technical Procedures
EXSUM	Executive Summary
FAR	Federal Acquisition Regulation
FPCON	Force Protection Condition
FRAGO	Fragmentary Orders
FRD	Functional Requirements Document
GFP	Government-Furnished Property
GTC	Global Ticketing Consolidation
IA	Information Assurance
IAM	Information Assurance Management
IAT	Information Assurance Technical
IATO	Interim Authority to Operate
IAPM	Information Assurance Program Manager
IAVA	Information Assurance Vulnerability Alert
IAVM	Information Assurance Vulnerability Management
IAW	In Accordance With
IDAM	Identity and Access Management
IMO	Information Management Officer
IPR	In-Progress Review
IS	Information Systems
ISSM	Information Systems Security Manager
ISSO	Information System Security Officer
ISSP	Information System Support Plan
IT	Information Technology
ITIL	Information Technology Infrastructure Library
ITSM	Information Technology Service Management
JPAS	Joint Personnel Adjudication System
JWICS	Joint Worldwide Intelligence Communication System
KM	Knowledge Management
KO	Contracting Officer

LCM	Lifecycle Management
LDAP	Lightweight Directory Access Protocol
LWN	LandWarNet
NACLC	National Agency Check with Law and Credit
NEC	Network Enterprise Center
NETCOM	Network Enterprise Technology Command
NIPR	Non-classified Internet Protocol
NIPRNet	Non-secure Internet Protocol Network
NIST	National Institute of Standards and Technology
OCI	Organizational Conflict of Interest
OCONUS	Outside Continental United States (includes Alaska and Hawaii)
OPORD	Operations Order
OPSEC	Operations Security
OPT	Operational Planning Team
P/C/S	Post, Camp, Station
PHI	Protected Health Information
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
PM	Program Management
POA&M	Plan of Action and Milestones
POC	Point of Contact
PPSM	Ports, Protocols and Services Management
PWS	Performance Work Statement
QA	Quality Assurance
QASP	Quality Assurance Surveillance Plan
QC	Quality Control
QCP	Quality Control Plan
RFC	Request for Change
RMF	Risk Management Framework
SCI	Sensitive Compartmented Information
SDP	Service Design Plan
SIMS	Security Information Management System
SIPR	Secret Internet Protocol
SIPRNet	Secure Internet Protocol Network
SITREP	Situational Report
SME	Subject Matter Expert
SOP	Standard Operating Procedure
SQL	Structured Query Language
SS	Service Support
SSBI	Single Scope Background Investigation
SSM	Service Support Module
STIG	Security Technical Implementation Guide
TA	Technical Authority
TCO	Telephone Control Officer
TDY	Temporary Duty
TTP	Tactics, Techniques and Procedures
UG	User Guide
VPN	Virtual Private Network

VTC	Video-Teleconference
WEM	Wireless Enterprise Management
WP	White Paper
XML	Extensible Markup Language

Attachment A

Performance Requirements Summary

PWS Paragraph	Required Services	Performance Standards	Acceptable Quality Level	Incentives /Disincentives for Meeting or Not Meeting Performance Standards
C.3.16.	Connect VTC Systems	Connect VTC systems by the agreed timelines	VTC systems are connected by the agreed timelines 98% of the time	Positive and negative performance will be documented in monthly COR reports.
C.3.18.	Provide Security Compliance Report detailing enterprise systems and applications are in compliance with Security Technical Implementation Guides (STIG) and Information Assurance Vulnerability Alerts (IAVA) patches and updates.	Reports are provided weekly by the due date and by the agreed timeline as tasked	Weekly reports are provided by the due date 100% of the time and by the tasked agreed timeline 98% of the time	Positive and negative performance will be documented in monthly COR reports.
C.3.18.	Provide review and development of Service catalogs,	Reviews and deliverables are	Reviews and deliverables are	Positive and negative performance will be

PWS Paragraph	Required Services	Performance Standards	Acceptable Quality Level	Incentives /Disincentives for Meeting or Not Meeting Performance Standards
	design packages, and support modules	provided by the due date	provided by the due date 98% of the time	documented in monthly COR reports.
C.3.18.	Provide system COOP draft and updates	Drafts and updates are provided by the agreed timeline	Drafts and updates are provided by the agreed timeline 98% of the time	Positive and negative performance will be documented in monthly COR reports.
C.3.19	Provide review and development of associated Capability Management documents, requirements, procedures, plans, and schedules.	Reviews and deliverables are provided by the due date	Reviews and deliverables are provided by the due date 98% of the time	Positive and negative performance will be documented in monthly COR reports.
C.8.6.	Contractor personnel will maintain current IT access and IA certification requirements.	Contractor personnel have current IT access and IA certifications.	Contractor personnel have current IT access and IA certifications 98% of the time.	Positive and negative performance will be documented in monthly COR reports.