PERFORMANCE WORK STATEMENT (PWS)

FOR

EDGEWOOD CHEMICAL BIOLOGICAL CENTER (ECBC) CHIEF INFORMATION OFFICER (CIO)
TECHNICAL AND STAFF SERVICES SUPPORT/CYBER SECURITY (CS) SUPPORT

1.0 PERFORMANCE WORK STATEMENT:

1.1 INTRODUCTION: The Research Development Engineering Command, Edgewood Chemical Biological Center, Chief Information Office (RDECOM, ECBC CIO) is a Research Development Test & Evaluation (RDT&E) organization with a unique mission supporting its researchers, developers, scientists, and information security to ensure decisive capabilities for unified land operations to empower the Army, the joint warfighter and our nation as well as to provide innovative solutions to counter Weapons of Mass Destruction threats.

1.2 OBJECTIVE: The objective of this task order is to provide Technical and Staff Services Support/Cyber Security (CS) Support of systems and Staff Support Services fulfilling the ECBC CIO/RDECOM G-6 mission.

1.3 BACKGROUND: As security threats, technology and communication capabilities increases, ECBC CIO/RDECOM G-6 requires a more holistic approach to development and configuration with a primary focus on integrated security. ECBC CIO/RDECOM G-6 has a need for IT RDT&E mission services at the IT enterprise level. This IT enterprise requires contract personnel with a specific and deep knowledge of security procedures, tailored experience, and certifications with a requirement for high level expertise in switch and router configuration, the knowledge of security requirements and ability to focus on large footprint and the integration of multiple systems. Security requirements include numerous certifications and the ability to provide a depth and reach-back capability to handle evolving cyber security requirements. Cybersecurity (IA/CS) System Security Engineering, and Support (SSES) support services are necessary to satisfy the goals and objectives for Emergency Management Systems, Army Financial Management Systems as well as Disaster Recovery and Continuity of Operations Planning that are inherent components of the IT enterprise.

1.4 SCOPE: The RDECOM ECBC DREN network is a R&D network, the enterprise currently consists of over 200 network switches, routers and other security appliances, plus over 100 WAP (Wireless Access Points). There are 160 Windows Servers and 50 Linux Servers including both SQL and Oracle databases. We also support a large SharePoint presence supporting over 3000 customers with custom designed applications. There are approximately 2200 Windows workstations including over 250 thin clients utilizing Citrix. The enterprise consists on both classified and unclassified networks. The contractor will be required to support the ECBC CIO/RDECOM G-6 mission and all related missions supported by the ECBC CIO. ECBC CIO/RDECOM G-6 is responsible for conducting and synchronizing operations across the Defense Research and Engineering Network (DREN) spectrum in support of the Army to ensure the availability, integrity, and confidentiality of the information and information systems used by the RDT&E community. ECBC CIO/RDECOM G-6 provide services for the protection, monitoring, analysis, detection and response to unauthorized activity within the DREN. Services are required to defend against unauthorized activity on the supported network Defense Research and Engineering Network (DREN). This includes activities from simple external hackers who may attempt to gain unauthorized access, insider threats attempts for unauthorized access, and policy violations that may impact network security and operations, and more. The contractor shall provide intelligence support to cyber operations, including contingency operations and exercises, to include research, evaluation analysis, integration, and interpretation of information from multiple intelligence and operational sources, and fuse the information into finished intelligence products for anticipated or unspecified intelligence production requirements. The contractor shall develop reports and products, both current and long-term in support of the ECBC CIO/RDECOM G-6 mission.

1.5 PERIOD OF PERFORMANCE (POP): Period of performance will for a Base period of one year and four year option periods. Total duration of award including option periods, is not to exceed 5 years.

2.0 APPLICABLE DOCUMENTS:

2.1 Government Document

- NARA Bulletin 91-4, National Archives and Records Administration
- AR 25-400-2 The Army Records Information Management System (ARIMS), 2 October 2007
- AR 25-1 Army Information Technology, 25 June 2013
- AR 25-2 Cybersecurity , 24 October 2007
- DoD Instruction 8500.01, Cybersecurity, 14 March 2014
- DoD Instruction 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT), 12 March 2014
- DoD Directive 8140.01, Cyberspace Workforce Management, 11 August 2015
- DFAR 48 Code of Federal Regulations Part 252.204.7012, Safeguarding Unclassified Controlled Technical Information (UCTI)
- DFAR Case 2006-D023 Cybersecurity Contractor Training and Certification

2.2 Non-Government Documents

- A Guide to the Project Management Body of Knowledge (PMBOK® Guide), Project Management Institute (PMI), latest edition
- Government Extension to the PMBOK® Guide Third Edition, PMI, September 2006
- IT Service Management, Information Technology Infrastructure Library V3, (http://www.itil-officialsite.com/home/home.asp)
- Electronic Industries Association (EIA)/ Institute of Electrical and Electronics Engineers (IEEE) J-STD-016-1995 Standard for Information Technology Software Life Cycle Processes, Software Development Acquirer-Supplier Agreement
- IEEE/EIA 12207.0-1996, Software Life Cycle Processes, 2 Mar 1998
- IEEE STD 1219-1993, IEEE Standard for Software Maintenance, 2 June 1993
- Warranty information American National Standards Institute/Electronic Industry Association (ANSI/EIA) publication 748-98

3.0 TASK REQUIREMENTS

This PWS describes the current ECBC CIO/RDECOM G-6 IT Technical and Staff Services Support/Cyber Security (CS) Support requirements.

All contractor personnel performing work shall be experienced professionals and acceptable to ECBC. The candidates' specific qualifications shall be clearly demonstrated and documented. The following matrix summarizes the required certifications and clearances per task. More detail is provided in the specific task areas.

	Comp TIA A+ (CE)	Comp TIA Security+ (CE)	Comp TIA Network+ (CE)	Computing Environment (CE) Cert.	Secret Clearance*	Top Secret (TS) Clearance	Other	Comments
3.1 Project Management Support					X		X	PMP cert (Desired)

3.2 System Administration Support		X		X	X	X		Minimum of 3 TS FTEs required at task award; CE Cert shall be obtained within 6 months of appointment.
3.3 Network Engineering/Operations/Management Support		X	X	X	X	X	X	Security+ OR Network+ acceptable; Minimum of 2 TS FTEs required at task award; Cisco CCNA, or equivalent required; CE Cert shall be obtained within 6 months of appointment.
3.4 Information Assurance Support (Technical and Managerial)		X		X		X		All FTEs are required to have TS at task award
3.5 SharePoint Administrator		X		X	X			CE Cert shall be obtained within 6 months of appointment.
3.6 Business Analyst Support (Optional Task)					X			
3.7 Sharepoint Solutions Architecture/Development		X		X	X			CE Cert shall be obtained within 6 months of appointment.
3.8 Privacy Officer (Optional Task)					X		X	Certified Information Privacy Technologist (CIPT) and Certified

								Information Privacy Professional (CIPP) required
3.9 IT Facilities Support					X			
3.10 Graphics Designer/Visual Information Support (Optional Task)					X			
3.11 Knowledge Management Support (Optional Task)					X			
3.13 Warehouse Manager					X			
3.14 Warehouse Technician	X			X	X			CE Cert shall be obtained within 6 months of appointment.

*Interim Secret is allowed until full Secret clearance is granted.

Customer support timeline – Standard baseline customer support is to be provided within 4 business hours of request. VIP (A VIP) defined as a GS-15, COL/CAPT (O-6), SES or General Officer (GO) support shall be provided to GS 15 positions or higher will be provided within one business hour of the request.
Contractor personnel filling a technical role that requires a baseline certification by DoD or Army regulation shall possess baseline certifications at the time of initial employment that satisfies the IAT II level and shall stay current with any and all additional or emerging required certifications during the entire life time of the task award. Contractor personnel are responsible for maintaining all relevant certifications throughout the term of their employment under this contract. Failure to maintain current certifications may be cause for termination of employment.

To account for the possibility that the Government's requirements may increase at a faster rate than currently projected, the Government reserves the right to increase the estimated overall ceiling value of this Task Order by as much as 30% over the life of the Task Order (TO), if necessary. Such increases shall only apply to additional effort that clearly falls within the scope of the Performance Work Statement and within the performance period of the TO, including all available option periods.

Fluctuations in the Government's requirements over the life of the task order are difficult to project at this time given uncertainties with the PM MC organizational structure and how it may impact the IT services required in support of this task order. If support is required, the Government will specify the scope, timeline, and extent of such requirements post-award. It is expected that Contractor will scale support (expands or contract resources) to provide appropriate staffing levels to meet the government's emerging needs while maintaining approved post

award service Levels. The ceiling value of the task order will be adjusted to accommodate the potential increases or decreases associated with such change.

Vacancy: Any FTE position from the time of award that is not staffed will be considered a vacancy. The Contractor must immediately notify the COR when a FTE is or will become vacant, for any reason to include employee resignation, reassignment within the company, or other condition creating a vacancy. The Contractor must replace vacant FTE(s) within 30 calendar days. Vacancies in excess of 30 calendar days will be assessed a vacancy reduction for each billing period the FTE is vacant. Vacancies in excess of 30 days created by circumstances or conditions outside the control of the contractor will not be assessed a reduction. The vacancy reduction is in addition to the contract incremental FTE monthly price reduction. The vacancy reduction is 20% of the contract incremental FTE monthly price. Vacancy accounting starts 30 calendar days after contract award, or 45 calendar days after any modification which increases FTE.

3.1 PROJECT MANAGEMENT SUPPORT:

The contractor shall provide qualified and experienced project management support utilizing industry best project management practices (Project Management Body of Knowledge (PMBOK®) Guide), which include all of the tasks required to initiate, plan, manage, control, report and close-out this task order. The Contractor shall participate in integrated project teams and develop project plans, Work Breakdown Structure (WBS), activity schedules, GANTT charts, Pareto diagrams, PERT charts, and project status reports utilizing standard software tools adopted by ECBC (Microsoft Suite, i.e. Project, Word, PowerPoint, Excel).

The Contractor shall provide overall management and oversight of all projects performed by contractor personnel, to satisfy the requirements identified in this Performance Work Statement (PWS). This includes coordinating with multiple teams within the ECBC CIO to ensure all projects are planned and executed across the entire enterprise. Keep the CIO team leads or TPOC's informed of project status as defined with this PWS. The contractor shall develop reports and products that document both current and long-term support of the ECBC CIO/RDECOM G-6 mission.

- The Project Manager shall be responsible for the Quality of all personnel and Services provided under this contract. This shall include responsibility for: Ensuring quality of services, products and personnel on time and within budget IAW the contract, to include meeting the approved post award Service Levels
- Validating the Quality System is compliant with the requirements of the contract whether it's a Quality Control Plan (QCP) or a Quality Management System (QMS)
- Conducting Quality inspections that ensure services, products and personnel are acceptable and ready for government acceptance
- Implementing a system which stresses prevention of non-conformance rather than correction of non-conformance
- Implementing a system to address customer complaints and corrective action requests

Task for Project Management Support:
The Contractor shall:

- Ensure that all projects performed meet the PWS requirements within the funding, timing and staffing constraints of the task order.
- Work closely with the Technical Point of Contacts (TPOC) to facilitate effective planning and accomplishment of critical objectives in a timely manner. Provide weekly project status updates, either verbally or in writing.
- Support the TPOCs by providing information related to the performance and completion of the tasks identified in the PWS.
- Attend all formal project reviews as well as all periodic progress meetings scheduled by the TPOC
- Notify the TPOC of any delays, problems or issues that may occur with specific projects
- Ensure that all projects performed are coordinated through the Change Management Control Board and all Request for Change are submitted in accordance with ECBC/RDECOM G-6 policy.
- Implement the Contractor's Quality Assurance plan

The Project Manager shall serve as the point of contact for interaction with the TPOC regarding all related issues to the requirements.

The Project Manager shall be the focal point for Continual Process Improvement recommendations to the Government that originate from the Contractor's staff. These recommendations could include changes to processes, introduction of tools to improve efficiency, or the introduction of new IT capabilities for mission support.

The Project Manager shall provide implementation plans to the TPOC for large scale deployments of IT projects across multiple teams. The Contractor shall ensure the deployment plan includes additional software and hardware tools and methods to facilitate efficient deployment. The Project Manager shall monitor and report to the TPOC the performance standards against the performance metrics as stated in the agreed upon within the PWS. The Project Manager shall oversee and execute the approved deployment plan. The project manager shall coordinate with the TPOC to provide any hardware or software required for the execution of the plan.

POST AWARD SERVICE LEVEL AGREEMENTS (SLA)

It is the intent of the Government to significantly improve the quality and consistency of the end-user IT services delivered over the life of this task order. To that end, it is the intent of the Government to move into a Service Level Agreement (SLA) based operation.

Within thirty days of award, the contractor shall propose initial service level agreements for this task order. The extent of these post award SLAs shall be to improve upon the metrics as stated in PWS section 13 - Performance Requirement Summary/Quality Control Plan (QCP). The contractor shall develop an initial list of SLAs along with the appropriate monitoring and reporting structure. This initial SLA list will become the baseline of an on-going Service Management program. The contractor shall monitor and report against this initial set of SLAs for the initial 6 months of the task order. At the end of 6 months, the contractor shall recommend a base level of acceptable performance, not to be less than the average performance for each measure recorded during the initial 6 months, for each of the service measurement areas. The Government shall provide feedback to the proposed SLAs and require revisions as necessary.

The contractor shall propose Service Levels to be achieved over the course of this task order. Proposed Service Levels shall be identified for the following key services:

- Computing/Data Center Services

- Network Services
- Cyber and Information Assurance Support Services
- Application Development and SharePoint Services

The contractor shall use the format in Table 1 (see below) or an updated table that the Government provides post award for the initial structure of Service Level documentation. This structure shall be refined over the course of the task order upon mutual consent of the contractor and the Government. The descriptions for the Columns of the Table are:

Service Level (SL) Title: This is the common title of the service level measure defined.
SL Explanation: service level description defining what is measured and why
SL Objective: the units of measure (e.g., hours, %, days, minutes, etc.) and ultimate target, (i.e., minimize, maximize, etc.)
SL Metric: the actual level of service required
SL Responsibilities: brief allocation of key responsibilities between contractor and government
SL Assumptions on how it will be calculated: the proposed algorithm to be used and key assumptions on availability of specific data

The following SLA are incorporated via 3Vesta's Quality Control Plan, dated July 31, 2016:

(b) (4)

[redacted]

(b) (4)

[redacted]

(b) (4)

[redacted]

(b) (4)

[redacted]

(b) (4)

[redacted]

The contractor shall identify the scope, the proposed metrics, the methods and algorithms used to calculate the metrics, timeliness of reports, methods of reporting, and all variables identified in adjusting the results to create the Service Level measure. The proposed Service Levels shall be incorporated into the task order, shall be binding upon the contractor, and shall be the baseline for continuous improvement initiatives throughout the life of the contract.

The Contractor shall propose appropriate changes with supporting rationale to the Service Level Measures and Metrics every six months. Changes shall be reviewed by the Government and, if accepted, implemented within 60 days of acceptance. If proposed changes are not accepted, the Contractor shall continue to use the Service Level Measures and Metrics currently in force.

Service Level Non-compliance: The terms of service level non-compliance shall be mutually agreed upon post award.

3.2 SYSTEM ADMINISTRATION SUPPORT:

Personnel at a minimum, shall have the following:.

- Security Clearance level - Interim Secret is allowed until full Secret clearance is granted. Top Secret may be required on a case by case basis as determined by the TPOC.
- Minimum of 3 contractors require Top Secret clearance at task award.
- Within 6 months of appointment employee shall obtain a computing environment certification relevant to job duties, subject to discretion of organization Information Assurance Manager (IAM).
- Contractor personnel filling System Administrator (SA) or Network Administrator (NA) roles shall possess a DoD 8570.01-M baseline certification (same as Security + certification) at the time of initial employment that satisfies the IAT II level during the entire life time of the task award.

The Contractor shall ensure the ECBC Enterprise Windows Server System is fully functional twenty-four hours a day/seven days a week. In the event that there is down time, the Contractor shall troubleshoot, resolve the problem and recover the ECBC Enterprise Windows Server System to maximum performance in the shortest amount of time as possible.

The Contractor shall:

- Ensure that the ECBC Enterprise Windows Server System meets all DoD 8500 series security requirements.
- Implement and monitor the ECBC Enterprise Windows Server System backup and restore operations as defined within existing SOP's provided by the government.
- Provide development of systems architecture and other system engineering/administration documentation.
- Create test plans to allow for a proper evaluation of hardware and software being considered for implementation.
- Provide written evaluations of system concepts, system designs, and system support program proposals with the goal of recommending actions for optimizing system performance to include evaluations of technical and production performance.

- Implement and monitor the ECBC Enterprise Windows Server System disaster recovery plan.
- Implement and monitor the ECBC Enterprise Windows Server System testing and installation of patches, updates, additional tools and future versions of all software on a daily basis.
- Ensure the ECBC Enterprise Windows Server System daily logs are kept on the ECBC Enterprise Windows Server and are provided to the ECBC IAM (Cybersecurity Manager) upon request
- Troubleshoot all IT issues for the assurance of the ECBC Enterprise Windows Server System server reliability.
- Provide recommendations to the TPOC that address the future performance needs of the Enterprise Windows Server System through ongoing monitoring of capacity planning and management for the continuity and functionality of the system operations and integration.
- Perform full beta-testing to ensure full functionality and integration with all ECBC Enterprise Windows Server systems prior to applying changes to production systems.
- For new projects or systems, the contractor shall provide the TPOC with written test plan for approval prior to implementation. The TPOC shall approve the plan within one week of receipt. The Contractor shall provide written testing results prior to putting systems into production.
- Perform preventative maintenance and server patching after normal business hours with approval from the Project Manager.
    - Schedule installation of all required server patches to occur after normal business hours (see section 9.0 for hours of operation). The Contractor shall install patches manually on the Windows Enterprise Server Environment.
    - Upgrade, maintain and provide security patches on all ECBC CIO/RDECOM G-6 servers in this environment. Ensure compliance with Cybersecurity Vulnerability Alerts (IAVAS) and Security Technical Implementation Guides (STIGS).
- Control the organization's data resources, which include managing multiple relational databases and servers.
    - Provide database design, and implement security systems solutions that will provide detection, prevention, containment, and deterrence mechanisms to protect and maintain the integrity of data files.
    - Maintain the integrity of the data, recover corrupted data and eliminate data redundancy.
    - Optimize database performance.
    - Provide support for Oracle, Wordpress, Sybase, MicroSoft Structured Query Language (SQL) Server or as needed for other relational databases.
    - Work with the applications development teams(s), and focus on the back-end portion of data storage and performance considerations for application systems being developed.
    - Design, implement, administer, and maintain databases in integrated, virtual, grid architecture.
- Provide System Administration of VMWare Products (e.g. ESXi 3.5, VSphere 4.0, VMWare Center), Storage Area Networks, and for DELL and HP hardware platforms.
- Administer system security tools (e.g. Symantec End Point Protection, NTP, AV, and McAfee Solidcore).

- Administer Active Directory, (Windows Server Update Services) WSUS, (Microsoft Operations Manager) MOM, Citrix, (Virtual Desktop Infrastructure) VDI, (Dynamic Host Configuration Protocol) DHCP, (Dynamic Name Server) DNS, Print Server's, File Server's, Veritas, and Microsoft clustering.
- Provide engineering consulting and compliance management as required by government policy.
- Assist in technical evaluation of the vendor submissions for compliance with government defined specifications.
- Prepare and present training information to the Project manager or technical staff and user personnel.
- Maintain systems and data integrity that includes virus checking. Ensure maximum availability and performance given resources.
- Optimize system layout and monitor capacity restraints. Monitor and administer database security, create and administer user accounts. Monitor, troubleshoot, and maintain the database.
- Backup and recover the database.
- Configure database network services.
- Interpret and write SQL queries and coach developers in SQL scripting. Also, develop and execute queries for ad-hoc retrievals and data mining.
- Support application development and testing to include: the review of application data models and database designs (logical & physical) with developers suggesting efficiencies where appropriate.
- Provide support for file backup systems, including the Network Appliance/Veritas Spectralogic system. Provide/oversee independent backup for designated systems. Produce mirrored copies of tapes for off-site storage. Coordinate storage of tapes with librarian. Provide emergency recovery tape backups for all servers.
- Provide full support for administering a variety of Operation systems: Linux, VMware, Apple MAC and IOS, Android, Windows servers, Citrix server including web application and backups, and other operating systems.
- Provide support for administering Wordpress and Oracle systems
- Manage authentication and permissions including eDirectory and Single Sign On (SSO) Support. Liaison with connected agencies.
- Participate in Change Management Control process and submit Request for Change in accordance with ECBC/RDECOM G-6 policy.
- Maintain ECBC's Citrix environment for both thin clients and remote access as directed by the TPOC.
- Provide IT support for IP base VTC system

3.3 NETWORK ENGINEERING/OPERATIONS/MANAGEMENT SUPPORT:

Personnel at a minimum, shall have the following:

- Within 6 months of appointment employee shall obtain a computing environment certification relevant to job duties, subject to discretion of organization Information Assurance Manager (IAM).

- Contractor shall possess a Cisco CCNA (Cisco Certified Network Associate) or equivalent as approved by the TPOC.

- Contractor personnel filling Network Administrator roles are to possess a DoD 8570.01-M baseline certification that satisfies the IAT II level prior to appointment.

- Interim Secret is allowed until full Secret clearance is granted. Top Secret may be required on a case by case basis as determined by the TPOC.

- Minimum of 2 contractors require Top Secret clearance at task award.

The Contractor shall provide network engineering support in the areas of design, installation, reconfiguration and testing of network architectures to manage and maintain an unclassified and classified network infrastructure utilizing state-of-the-art, cutting edge technology. The Contractor shall research and recommend solutions for new equipment, software, network configuration and management, in order to support all ECBC networking requirements. The Contractor shall keep up-to-date records and documentation of network topology and equipment configurations to support network status reports, network troubleshooting, and network logging. The Contractor shall configure the routers, firewalls and switches following the TPOC direction for allowing specific ports and protocols.

The Contractor shall configure the Virtual Private Network (VPN) concentrator and Virtual Local Area Networks (VLAN) at the direction of the TPOC. The Contractor shall test, evaluate and incorporate new technology as they are developed in the industry and approved by the TPOC. The contractor shall configure, install or move network equipment that communicates via fiber optic cable utilizing both Single Mode and Multi-Mode (62.5 micron) to communicate within the ECBC enterprise network.

The Contractor shall provide network monitoring utilizing ECBC's network and server monitoring tools. The Contractor shall provide patch management and backup configuration for all network routers and switches. All routers and switches shall be kept compliant with the appropriate Cybersecurity Vulnerability Alert (IAVA) software and manufacturer patches. Router and switch configurations shall be backed up weekly and previous versions will be maintained for a period of six months. The Contractor shall install pre-manufactured patch copper cables and optical fibers required to support user's data communication requirements. This requirement involves running copper and fiber optic cables, patching the cables with appropriate jacks or connectors, testing the work for proper operation, and keeping records of the work that was accomplished. The Contractor shall remedy network faults and perform diagnostic tests on the network components using portable testers, fixed network monitoring stations and software contained in network devices. The contractor shall remediate all network issues and perform actions to restore proper operations. Typical corrective tasks include replacing copper or fiber optic patch and adjusting configuration of network communications or routing devices via switches. The Contractor shall install, remove, configure and repair encryption equipment to alter, expand or maintain the ECBC secure computer network used for classified processing. Knowledge or formal training on Communications Security (COMSEC) accounting or handling policies is necessary for any support of the classified computer networks.

The Contractor shall manage the Internet Protocol (IP) addresses in the ECBC IP address space. The Contractor shall maintain IP address records in the ECBC IP Host List for both static and Dynamic Host configuration Protocol (DHCP) addressing. The Contractor shall maintain each record for completeness, accuracy and assure that each IP address is actively used or appropriate action is taken to have the IP removed from the IP Host List. The Contractor shall also maintain a DHCP server device as appropriate.

The Contractor shall research, develop, demonstrate, integrate, and test innovative technologies that defend against cyber security threats. The contractor shall provide recommendations and develop SOP's for all accepted and approved solutions that will help protect against cyber security threats.

The Contractor shall manage the ECBC Wireless infrastructure including Wireless Internet (WiFi) network, ensuring that the wireless controller and WAP's (Wireless Access Points) are managed and monitored. The Contractor shall review all logs to ensure that the WiFI network remains protected. The contractor shall

monitor the WiFi network looking for rouge devices and shall inform the TPOC if any of these devices are discovered. The Contractor shall ensure that the Broadcast Standard Software Interface Definition (SSID) is disabled and that all (Wireless Access Points) WAP's are set to use WPA2 AES security and have the appropriate STIG configurations installed.

Task for Network Engineering/Operations/Management Support:
The Contractor Shall

- Install, support and maintain new network hardware and software for the ECBC infrastructure.
- Implement enterprise network policy and maintain cyber security initiatives and directives as directed by the TPOC.
- Provide technical and programmatic support to assist other ECBC teams and supported organizations in all aspects of planning, engineering, fielding and operating IT systems and resources.
- Perform efficient and effective performance-based network engineering services in the following areas of research, development, test and evaluation: systems, affordability/failure analysis; experimental testing, data acquisition and reduction, hardware design and development, risk assessment; consulting and configuration management.
- Implement, administer, maintain, and configure the ECBC network to monitor, detect, and respond to threats on the network
- Maintain a VPN and optimize network access to remote disaster recovery site.
- Configure, manage and utilize Intrusion Detection system (IDS)/Intrusion Prevention system (IPS) to detect and prevent threats to the ECBC environment, and uncovering potential vulnerabilities in the network. The contractor shall then review these potential vulnerabilities/threats, update sensor baseline signatures (minimizing false positives) and provide recommendations and potential solutions to these threats to the TPOC.
- Conduct persistent penetration and vulnerability testing as described US Army Cybersecurity Wireless Security Standards Best Business Practices v 4.0 or later.
- Assess new technologies and devices upon request by the TPOC. The contractor shall determine if technology or device will support/satisfy new requirements, positively enhance the analysis process and security posture of the network, integrate into existing architecture and tools sets, and can properly be accredited and authorized for use in the current environment.
- If there are immediate threats to the network and systems are detected, the contractor shall immediately brief the TPOC of these issues.
- Review and update all SOP's annually
- Manage network equipment including Routers, Citrix Netscaler, Cisco/Brocade switches, Firewalls and associated peripherals.
- Maintain permissions and passwords and proper level of access to network infrastructure.
- Monitor network usage.
- Suggest and provide IT solutions to improve network performance.
- Ensure that all equipment is based on current industry standards including any new or emerging technologies.
- Plan and implement future network upgrades as directed by the TPOC
- Participate in Change Management Control processes and submit Request for Change in accordance with ECBC/RDECOM G-6 policy.

- Provide IT support for IP base VTC systems.
- Install, remove, configure and repair encryption equipment to alter, expand or maintain the ECBC secure computer network used for classified processing. Knowledge or perform formal training on Communications Security (COMSEC) accounting or handling policies is necessary for any support of the classified computer networks.
- Network Engineering Support is also required for ECBC customers at Dugway Proving Ground and the Army Materiel Systems Analysis Activity (AMSAA) .

*Task for **Network Engineering/Operations/Management Support** (Master):*

CERTIFICATION REQUIREMENTS: ISC2 CISSP or other IAM-III DoDI 8570.01-M baseline certification AND DoDI 8570.01-M IAT-II computing environment certification for privileged level access to DoD Information Systems
CLEARANCE REQUIREMENTS: SECRET with the eligibility to obtain TOP SECRET and or TOP SECRET SCI
FUNCTIONAL RESPONSIBILITY: Performs a variety of network engineering tasks, independently, which are broad in nature and are concerned with the design and implementation of integrated networks, including personnel, hardware, software and support facilities and/or equipment. Supervises team of Network Engineers through project completion. Plans and performs network engineering research, design development, and other assignments in conformance with network design, engineering and customer specifications. Supervises Network Engineers through project completion. Responsible for major technical/engineering projects of higher complexity and importance than those normally assigned to lower level engineers. Performs with great latitude for unreviewed actions and decisions. Coordinates the activities of Network Engineers and Network Technicians assigned to specific network engineering projects. Provides technical/management leadership on major tasks or technology assignments. Establishes goals and plans that meet project objectives. Has domain and expert technical knowledge. Directs and controls activities for a client, having overall responsibility for financial management, methods, and staffing to ensure that technical requirements are met. Interactions involve client negotiations and interfacing with senior management. Decision making and domain knowledge may have a critical impact on overall project implementation. May perform other duties as assigned.
MINIMUM EDUCATION: Advanced Degree in a relevant discipline or at least fifteen years of general experience of which twelve years is directly related experience, a degree is not required.

The Contractor shall:

- Determine enterprise DoD / Army Cybersecurity and security standards for the network.
- Develops and implement DoD /Army Cybersecurity/security standards and procedures on the network.
- Coordinate, develop, and evaluate the network for the organization or enterprise. Recommend DoD / Army Cybersecurity/security solutions to support customers' requirements.
- Identify, report, and resolve network issues in accordance with DoD and Army policy.
- Establish and satisfy DoD /Army Cybersecurity and security requirements based upon the analysis of user, policy, regulatory, and resource demands.
- Support customers at the highest levels in the development and implementation of doctrine and policies.
- Apply know-how to government and commercial common user systems, as well as to dedicated special purpose systems requiring specialized features and procedures.
- Perform analysis, design, and development of security features for system architectures.
- Analyze and define security requirements for the enterprise which may include mainframes, workstations, and personal computers.
- Design, develop, engineer, and implement solutions that meet DoD /Army security requirements.
- Provide integration and implementation network/computer system security solutions.

- Analyze general related technical problems and provides engineering and technical support in solving these problems.
- Perform vulnerability/risk analyses of enterprise during all phases of the system development life cycle.
- Ensure that the enterprise is functional and secure.
- Work autonomously to research and design solutions to satisfy customer requirements
- Proactively identify network security weakness and develop solutions to improve security posture.
- Provide project lifecycle management for network security driven efforts.
- Conduct research and fact finding to identify DoD/Army policies related to network security.
- Create, review and update Network Cybersecurity policies and documentation specific to the organization. Create, review and update security architecture documentation specific to the organization.
- Monitor the organization's network and can recognize suspicious or malicious traffic that is to be logged, and escalated appropriately.

3.4 CYBERSECURITY – SUPPORT (TECHNICAL AND MANAGERIAL):

Personnel at a minimum, shall have the following:

- Contractor personnel filling Cybersecurity roles are to possess a DoD 8570.01-M baseline certification that satisfies the IAM II level prior to appointment.

- All personnel security clearance level for this task section shall have a Top Secret clearance at task award. This is required for JWICS/SAP accreditation support.

- The Contractor shall provide a Senior Level Cybersecurity manager with experience in all aspects of DoD Cybersecurity.

The Contractor shall govern and monitor the security posture of the network enclave as well as provide authority on Cybersecurity policies that shall be adhered to from above the organization as well as internally made supplemental guidance. The Contractor shall work closely with organization's Government Cybersecurity Manager (IAM) in regards to policy creation, best business practices and general Cybersecurity (IA) Governance. The Contractor shall be the primary POC for all accreditation and inspection actions for the organization, and to serve as a Cybersecurity Manager Representative (IAM-R) for all IA actions required from higher headquarters.

The Contractor shall be responsible for all activities relating to Cybersecurity procedures and systems. The contractor shall develop information assurance programs and control guidelines. The Contractor shall confer with and advise subordinates on administrative policies and procedures and resolving technical problems, priorities, and methods. The Contractor shall consult with and advise other support teams within the ECBC CIO both contractor and government regarding internal controls and security procedures. The Contractor shall prepare activities and progress reports relating to the information systems audit function

Task for Cybersecurity*– Support (Technical and Managerial):*

The Contractor shall:

- Manage all steps of the new Certification and Accreditation (C&A) process and the Risk Management Framework (RMF). They shall have a working knowledge of Department of Defense Cybersecurity Certification (DIACAP)
- Create, develop and maintain the entire RMF executive package for every system.
- Create, develop and maintain a System Security Plan (SSP) for a network enclave.
- Assess all security controls as identified in Army regulation 25-1, 2 and DoD regulation 85xx series.
- Coordinate the implementation of Defense Information Systems Agency (DISA) field security templates to existing environment.
- Coordinate Cybersecurity C&A selection to the customer for reaccreditation phases.
- Create and maintain scorecard and Plan of Action and Milestones (POA&M) mitigation for accreditation packages.
- Manage organizational assets in all the DoD/Army asset portfolio management systems for system entry. These include, the C&A Tracking Database (Tdb) for accreditation, Federal Information security Management Act (FISMA) Cyberscope for all FISMA audit compliance taskers, knowledge of APMS for system justifications, etc.
- Perform Computer Security Incident Response activities for ECBC, coordinate with other Government agencies such as Army Computer Emergency Response Team (ACERT) to record and report incidents.
- Monitor and analyze Intrusion Detection Systems (IDS) to identify security issues for remediation.
- Recognize potential, successful, and unsuccessful intrusion attempts and compromises through reviews and analyses of relevant event logs and alerts received from servers, routers, firewalls and other appliances used to monitor the network.
- Evaluate firewall change requests and assess organizational risk.
- Communicate alerts to agencies regarding intrusions and compromises to their network infrastructure, applications, and/or operating systems.
- Assist with implementation of counter-measures or mitigating controls.
- Ensure the integrity and protection of networks, systems, and applications by technical enforcements and organizational security policies; and monitoring of vulnerability scanning software and devices.
- Perform periodic and on-demand system audits and vulnerability assessments, including user accounts, application access, file system and external Web integrity scans to determine compliance.
- Prepare incident reports of analysis methodology and results.
- Review vulnerability assessments and conduct gap analysis of assigned networks and systems.
- Develop a POA&M to address deficiencies.
- Perform required network patching to include vendor updates and Government directed patches; perform validation scanning as directed by applicable policy and guidance.
- Analyze audit security incident logs for individual or multiple network devices for unauthorized information and processes and unauthorized network access.
- Perform network security analysis and risk management for designated unclassified and classified networks.
- Provide guidance and work leadership to less-experienced technical staff members.
- Install and maintain security software programs.
- Train/instruct users and personnel on Cybersecurity and agency security guidelines..
- Ensure no information is illegally transmitted.
- Assist the cyber forensic experts in case of a breach in security.
- Provide written presentation recommendations in the areas of Cybersecurity to senior level managers.
- Provide a Change Manger to lead the Change Management Control Board in accordance with ECBC/RDECOM G-6 policy.

Task for Cybersecurity*– Support (Master):*

CERTIFICATION REQUIREMENTS: - ISC2 CISSP or other IAM-III DoDI 8570.01-M baseline certification AND DoDI 8570.01-M IAT-II computing environment certification for privileged level access to DoD Information Systems
CLEARANCE REQUIREMENTS: SECRET with the eligibility to obtain TOP SECRET and or TOP SECRET SCI
Provides technical/management leadership on major tasks or technology assignments. Establishes goals and plans that meet project objectives. Has domain and expert technical knowledge. Directs and controls activities for a client, having overall responsibility for financial management, methods, and staffing to ensure that technical requirements are met. Interactions involve client negotiations and interfacing with senior management. Decision making and domain knowledge may have a critical impact on overall project implementation. May supervise others.

The Contractor shall:

- Determine enterprise DoD / Army Cybersecurity and security standards.
- Developsand implement DoD /Army Cybersecurity/security standards and procedures.
- Coordinate, develop, and evaluate security programs for an organization. Recommend DoD / Army Cybersecurity/security solutions to support customers' requirements.
- Identify, report, and resolve security violations in accordance with DoD and Army policy.
- Establishe and satisfy DoD /Army Cybersecurity and security requirements based upon the analysis of user, policy, regulatory, and resource demands.
- Support customers at the highest levels in the development and implementation of doctrine and policies.
- Apply know-how to government and commercial common user systems, as well as to dedicated special purpose systems requiring specialized security features and procedures.
- Perform analysis, design, and development of security features for system architectures.
- Analyze and define security requirements for computer systems which may include mainframes, workstations, and personal computers.
- Design, develop, engineer, and implement solutions that meet DoD /Army security requirements.
- Provide integration and implementation computer system security solutions.
- Analyze general Cybersecurity-related technical problems and provides basic engineering and technical support in solving these problems.
- Perform vulnerability/risk analyses of computer systems and applications during all phases of the system development life cycle.
- Ensure that all information systems are functional and secure.
- Work autonomously to research and design solutions to satisfy customer requirements
- Proactively identify network security weakness and develop solutions to improve security posture.
- Provide project lifecycle management for network security driven efforts.
- Conduct research and fact finding to identify DoD/Army policies related to network security.
- Create, review and update Network Cybersecurity policies and documentation specific to the organization. Create, review and update security architecture documentation specific to the organization.
- Monitor the organization's network and can recognize suspicious or malicious traffic that is to be logged, and escalated appropriately.

3.5 SHAREPOINT ADMINISTRATOR:

Personnel at a minimum, shall have the following:

- Contractor personnel filling Sharepoint development roles are to possess a DoD 8570.01-M baseline certification that satisfies the IAT II level prior to appointment.

- Within 6 months of appointment employee shall obtain a computing environment (CE) certification relevant to job duties, subject to discretion of organization Information Assurance Manager (IAM).

- Security Clearance level - Interim Secret is allowed until full Secret clearance is granted. Top Secret may be required on a case by case basis as determined by the TPOC.

The Contractor shall manage all aspects of the SharePoint administration to include: availability, reliability, performance, monitoring, and security. The Contractor shall ensure that the ECBC Enterprise Windows Server System meets all current AR-25 series regulations as provided by the Task Manager upon task order award and during the task order performance. The Contractor shall work with the SharePoint and development teams, focusing on the back-end portion of data storage considerations and performance considerations for application systems being developed. The Contractor shall schedule installation of all required server patches to occur after normal business hours so that they do not disrupt the operational capabilities provided to the ECBC researchers through the IT infrastructure.

Task for SharePoint Administrator:
The Contractor shall:

- Provide SharePoint 2010 and 2013 Administration
- Provide SQL Server 2008/2012 administration
- Monitor Windows and SQL Cluster's performance, manage SharePoint development, quality assurance and staging servers
- Provide SharePoint environment planning, deployment and operational support
- Identify hardware and software issues for SharePoint and SQL servers and work with server admins to implement proper patches and updates
- Install and configure SharePoint servers
- Perform server/database migration between various SharePoint servers (2010/2013)
- Work with developers to deploy custom applications and solutions to production and pre-production environments.
- Coordinate with network services for Backup and Disaster Recovery plan for SharePoint environments, and verify testing of recovery plan
- Provide support to development team in server management, scripting, and access control.
- Maintain continuity of Web, SharePoint & SQL servers
- Satisfy all relevant Army clearances and training certifications.
- Participate in Change Management Control as required and submit Request for Change in accordance with ECBC/RDECOM G-6 policy.

3.6 BUSINESS SYSTEMS ANALYST SUPPORT (Optional Firm Fixed Price Task):

Personnel at a minimum, shall have the following:

- Security Clearance level - Interim Secret is allowed until full Secret clearance is granted. Top Secret may be required on a case by case basis as determined by the TPOC.

The Contractor shall support enterprise -wide financial and accounting systems reporting requirements. Data reports are to be generated based on data extracted from the General Fund Enterprise Business System (GFEBS). The Contractor shall be responsible for soliciting, organizing, understanding, reviewing, analyzing, and documenting, enterprise-wide financial accounting / reporting requirements, IT requirements, and requests that come from budget analysts, the business community, research and development programs, operations, and users of IT services. The Contractor shall assist with managing the implementation of solutions and shall be deeply involved throughout the solution development lifecycle in the capacity of business analyst and requirements subject matter expert, and is expected to take key responsibility and ownership for the requirements artifacts and the delivery of the solution. The Contractor shall have knowledge of business analysis, quality assurance, and workflow tools and/or practices and technology solution assessment and validation.

Task for Business Systems Analyst Support:
The Contractor shall:

- Provide analysis, definition, and direction in support of project activities.
- Act as the primary contact for technology, reporting, system integration, and process related analysis
- Interact with applicable budget and financial analysts, management, systems administrators, Database developers, and Project Managers to ensure adherence with scope management, change management, and solution definition
- Create functional specifications for new or modified systems and processes. Recommend system improvements.
- Conceptualize and design Dashboard solutions and reports that are representative of the business unit's productivity.
- Work with customers, project leads, software engineers, integration test team, and the quality assurance team to create documentation suitable for their use.
- Facilitates meetings and/or design sessions to validate, prioritize, and document specific requirements for application enhancements and/or new development.
- Gather and document business requirements, formulate use cases, track requirements, provide status, and ensure quality of solution throughout the project.
- Identify, assess, and record near-term business needs; recommending business priorities, and advising businesses on options, risks, and costs versus benefits.
- Support and/or facilitate business user systems training as needed.
- Act as interface between systems group and end users.
- Define, develop, and manage process improvement implementations.
- Perform project and program management activities as required.
- Participate in Change Management Control and submit Request for Change in accordance with ECBC/RDECOM G-6 policy.

Should this option be exercised, the service level agreement requirements of section 3.1 shall apply.

3.7 SHAREPOINT SOLUTIONS ARCHITECTURE AND DEVELOPMENT SUPPORT:

- Contractor personnel filling Sharepoint development roles are to possess a DoD 8570.01-M baseline certification that satisfies the IAT II level prior to appointment.

- Within 6 months of appointment employee must obtain a computing environment (CE) certification relevant to job duties, subject to discretion of organization Information Assurance Manager (IAM).

- Security Clearance level - Interim Secret is allowed until full Secret clearance is granted. Top Secret may be required on a case by case basis as determined by the TPOC.

The Contractor shall provide support services to develop, configure, monitor, and maintain SharePoint 2010 and SharePoint 2013 environments. The Contractor shall be responsible for overseeing architectural design and integration content management structure, portals, collaboration, business process or other solutions; They shall be instrumental in planning and implementing software version upgrade releases, troubleshooting and debugging SharePoint sites. The Contractor shall be proficient in analyzing information, SP architecture, and understand business requirements. Contractor shall possess relevant knowledge and experience in appropriate development tools for the web development in the Windows environment as well as Visual Studio, ASP.NET, JavaScript, Oracle and SQL Server databases.

Task for SharePoint Solutions Architecture and Development Support:
The Contractor shall:

- Be the lead on SharePoint customization projects and provide end-to-end enterprise Web application architecture and development.
- Support Sharepoint project design, development, planning, installation, configuration, monitoring, and maintenance of the SharePoint environment.
- Support development and maintenance of custom business applications.
- Provide development, installation, testing, and troubleshooting of new products from the concept phase onward, as well as taking complex and challenging existing systems and quickly developing expertise in maintaining and enhancing them.
- Mitigate all cyber security risks and information breaches by establishing and sustaining compliance, governance, and cyber assurance solutions for SharePoint.
- Comply and enforce Cybersecurity standards in the SharePoint environment.
- Work with the Cybersecurity team to ensure regular scanning of all data is conducted as directed by policy.
- Use metadata for discovery, classification, and security best practices.
- Implement solutions to securely share information between SharePoint servers and domains.
- Ensure permission policy compliance, and prevent security breaches and unauthorized access to sensitive content.
- Audit, clean-up and manage SharePoint permissions and users from a single console across all sites, site collections or farms.
- Maintain compliance, reduce risk and take control of what organization users can do in SharePoint with policy enforcement and control configurations for access privileges, use of versioning, file upload limits, site quotas and the use of site templates to mitigate all cyber security risks.
- Provide documentation for software architecture, software design and development.
- Provide development and maintenance of custom business applications.
- Support SharePoint architecture, functionality, configuration and branding.

- Document, update, and enhance processes and procedures and provide administrative actions as needed.
- Assist in the development and drafting of ECBC CIO/RDECOM G-6 Concept of Operations, policies and SOPs.
- Conduct all development and testing of systems prior to migrating to production
- Participate in planning the development and security cooperation and provide expert advice for documentation in support of cyber security.
- Maintain SQL accounts and change passwords as directed by the TPOC
- Create site architecture artifact to support requirements for all supported organizations
- Patch systems and comply with all cyber security regulations.
- Submit POA&M's as required
- Maintain third party solutions
- Meet all IAVA requirements addressing all vulnerabilities as directed by the IAM
- Maintain and document all configuration changes made to web front ends, application servers and backend SQL servers
- Support SharePoint configuration and maintain Organizational taxonomies, site collections, policies, procedures and solutions
- Prepare and document software (technical) requirements and specifications.
- Conceptualize and build new software design.
- Plan phases of the Software Development Life Cycle (SDLC).
- Conduct research on emerging application development software products, languages, and standards in support of "Build vs Buy" decision.
- Recommend, schedule, and perform software improvements and upgrades.
- Write, translate, and code software programs and applications according to specifications.
- Run and monitor software performance tests on new and existing programs for the purposes of correcting errors, isolating areas for improvement, and general debugging.
- Administer critical analysis of test results and deliver solutions to problem areas.
- Generate statistics and prepare and write reports for management and/or team members on the status of the programming process.
- Assist in the development and maintenance of user manuals and guidelines.
- Coordinate installation of software products for end users as required.
- Write programming scripts to enhance functionality and/or appearance of organizations web sites and/or related web applications as necessary.
- Remove code script from organization web sites and/or related web applications as necessary.
- Coordinate with network administrators, systems analysts, and software engineers to resolve problems with software products or company software systems.
- Design and develop highly scalable, usable, and distributed application using Microsoft .NET technologies
- Participate in Change Management Control and submit Request for Change in accordance with ECBC/RDECOM G-6 policy.

3.8 PRIVACY OFFICER (Optional Firm Fixed Price Task):

Personnel at a minimum shall have the following:

- Certified Information Privacy Technologist (CIPT) Certification
- Certified Information Privacy Professional (CIPP) Certification
- Security Clearance level - Interim Secret is allowed until full Secret clearance is granted. Top Secret may be required on a case by case basis as determined by the TPOC.

The contractor shall manage and oversee all ongoing activities related to the development, implementation and maintenance of, and adherence to the Organization's privacy policies and procedures. The contractor shall interface with TPOC /team leads to identify and implement privacy policies requirements.

Should this option be exercised, the service level agreement requirements of section 3.1 shall apply.

Tasks for Privacy Officer Support:
The Contractor Shall

- Provide development guidance and assist in the identification, implementation, and maintenance of organization information privacy policies and procedures in coordination with organization management.
- Perform ongoing compliance monitoring activities.
- Participate in the development, implementation, and ongoing compliance monitoring of all business associate agreements to ensure that all privacy concerns, requirements and responsibilities are addressed.
- Review all system-related information security plans throughout the Organization's network to ensure alignment between security and privacy practices, and acts as a liaison to the Information Systems Team members, if applicable.
- Work with all Organization personnel involved with any aspect of release of protected information, to ensure full coordination and cooperation under the Organization's policies and procedures and legal requirements
- Maintain current knowledge of applicable federal laws and accreditation standards, and monitor advancements in information privacy technologies to ensure organizational adaptation and compliance.
- Cooperate with the higher headquarters, other legal entities, and Organization and officers in any compliance reviews or investigations.
- Prepare and staff Privacy Impact Statements for the organization
- Participate in Change Management Control and submit Request for Change in accordance with ECBC/RDECOM G-6 policy.
- Have complete knowledge and understanding of the following Federal, DoD and Army Privacy regulations:
    - Title 5 of the United States Code, Freedom of Information Act (FOIA)
    - Section 208 of the E-Government Act of 2002, Pub. L. 107-347
    - DoD directive 5400.7, DoD Freedom of Information Act, Sept 1998
    - Department of the Army Pamphlet 25-1-1, (AR25-1) Army Information Technology Implementation Instructions, 25 June 2013
    - DoD Directive 5400.11, DoD Privacy Program, 14 May 2007
    - DoD Instruction 7650.01, Government Accountability Office and Comptroller General Requests for Access to Records, 27 Jan 2009
    - DoD Instruction 5400.16, Privacy Impact Assessment (PIA) Guidance, 12 Feb 2009

Should this option be exercised, the service level agreement requirements of section 3.1 shall apply.

3.9 IT FACILITIES SUPPORT

Personnel at a minimum, shall have the following:

- Security Clearance level - Interim Secret is allowed until full Secret clearance is granted. Top Secret may be required on a case by case basis as determined by the TPOC.

The Contractor shall under indirect supervision, assist in developing and monitoring assigned department acquisition, property accountability, mobile telecommunications and risk management efforts directly supporting

ECBC infrastructure IT goals and projects. The Contractor shall support ECBC CIO/RDECOM G-6 personnel in all aspects of Government purchasing via Government Purchase Card (GPC) and task order Purchase Requests (PR). The Contractor shall develop independent solutions to problems, and interfaces with other ECBC CIO/RDECOM G-6 team members and Government personnel to make decisions or recommendations to significantly enhance, interpret, or develop policies or programs.

Task for IT Facilities Support:
The Contractor shall:

- Manage configuration and support of all mobile devices used in ECBC and supported organizations
- Publish Standard Operating Procedures (SOPs), instruction manuals, and user guidelines via Microsoft SharePoint Portal.
- Use General Fund Enterprise Business System (GFEBS) at the User Access Level to create Purchase Requests (PR) to fund monthly data plan/cell plan invoices, IT acquisitions, and IT service contracts.
- Enter data, edit, proofread, organize and maintain various databases to include property inventory, acquisition requests, software licensing, Blackberry/mobile phone contracts.
- Coordinate and oversee the supply chain from vendor to customer for ECBC Commercial Off-The-Shelf (COTS) hardware and software purchases.
- Submit all required approval and waiver requests required for Army IT purchases, examples include CHESS Waivers, AKM Goal 1 Waiver requests, Agreements and Acceptance of Clauses, and Justifications for Other Than Full and Open Competition.
- Document all processes and procedures.
- Provide timely responses to and resolution of customer requests and problems.
- Schedule, coordinate, and oversee customer requests.
- Keep documentation up-to-date and filed.
- Provide guidance and work leadership to less experienced staff members.
- Work closely with other departments/organizations and collaborate with other IT Staff and Senior level personnel.
- Provide training and technical support for users with varying levels of IT knowledge and competence
- Satisfy all relevant Army clearances and training certifications.
- Contractor shall participate in Change Management Control and submit Request for Change in accordance with ECBC/RDECOM G-6 policy.

3.10 GRAPHICS DESIGNER/VISUAL INFORMATION SUPPORT (Optional Firm Fixed Price Task):

Personnel as a minimum shall have the following:

- Security Clearance level - Interim Secret is allowed until full Secret clearance is granted. Top Secret may be required on a case by case basis as determined by the TPOC.
- Knowledge in the most current design software (e.g. Adobe Creative Suite 6, Photoshop CS6, Illustrator CS6, Corel Draw X, Indesign CS6, Flash CS6, Acrobat 10 pro, 3ds Max 2012, Poser 7, Bryce 5IDVD).
- Knowledge in use of equipment (Mac & PC, Cintiq 21 UX, Cannon C1, HP6100 Printers, AGL 64T Laminator, AGL 64E Laminator, Gerber Edge FX, Gerber Envision, gunner F1.
- Strong background in publication, poster, brochures, fact sheets, newsletters, briefings, signage, and exhibition design.

Description of duties: The purpose of the Graphics Designer/Visual Information Specialist is to provide operating knowledge of personal computer (PC) and Macintosh based design and peripherals. This will include color lasers, color plotters, scanners, digital and video cameras, laminators, pre-press production, color separations, mechanicals, typography, color proofs/match prints, quality control and display art production. The specialists shall also be proficient with current software packages including Adobe CS (In Design, Photoshop, Illustrator, Acrobat) Quark Xpress, Corel Draw, PageMaker, Microsoft Office (Word, PowerPoint, Excel, Access, Visio) HTML and Multimedia. Conceptualize customer's initial idea and design with proficient execution, while presenting concepts and creative strategy to clients.

Tasks for Graphics Designer/Visual Information Support:
The Contractor Shall

- Conceptualize and design publications, posters, brochures, fact sheets, newsletters, briefings, signage, and exhibitions.

Be responsible for ensuring that files are print ready for Print Specialist. Should this option be exercised, the service level agreement requirements of section 3.1 shall apply.

3.11 KNOWLEDGE MANAGEMENT (KM) SUPPORT (Optional Firm Fixed Price Task):

Personnel as a minimum shall have the following:

- Security Clearance level - Interim Secret is allowed until full Secret clearance is granted. Top Secret may be required on a case by case basis as determined by the TPOC.

Tasks for Knowledge Management Support:
The Contractor Shall

- Maintain and manage knowledge system and database.
- Perform requirements analysis to determine KM solution.
- Interface with team leads to identify knowledge enhancement areas.

- Monitor and measure the establishment of new KM initiatives
- Interface with user community to determine knowledge requirements.
- Promote KM objectives, plans, and priorities to key audiences within the organization, helping to achieve adoption and leverage of the knowledge networks.
- Facilitate interaction between user community and functional teams.
- Coordinate KM initiatives
- Educate the organization on the use and benefits of KM, communities of practice, effective collaboration and long term corporate knowledge pools.
- Engage key stakeholders in the use and availability of KM networks and foster cross-network collaboration.
- Deliver key metrics, success stories, and use cases where KM has created and enhanced value for the organization.

- Facilitate the implementation and taxonomy of knowledge networks, coordinate taxonomy development, content development, and training materials.
- Develop metadata for tagging of organizations documentation.
- Improve search tools and techniques.
- Be responsible for KM strategies to improve the usability of information and knowledge
- Serve as the functional liaison on the KM program for both internal and external organizations.

Should this option be exercised, the service level agreement requirements of section 3.1 shall apply.

3.12 WAREHOUSE MANAGER

Personnel as a minimum shall have the following:

- Security Clearance level - Interim Secret is allowed until full Secret clearance is granted. Top Secret may be required on a case by case basis as determined by the TPOC.

Description of Duties: The contractor shall effectively maintain and manage the ECBC CIO Information Technology (IT) receiving warehouse and distribution operation in order to provide an efficient turn-around of orders. The contractor shall oversee and manage all Warehouse Technicians assigned to the ECBC CIO Receiving Warehouse. Duties include the receipt, barcoding, storage, and distribution scheduling of all IT-related hardware and software that is purchased by the ECBC CIO Acquisition Team. Maintaining 100% accountability of all products through the entire supply chain process. Accurate entry of receiving documents, hand receipt assignments, and delivery paperwork into the ECBC IT Warehouse Database. Overseeing the coordination of the imaging of all hardware with the ECBC Service Desk Imaging Team. Ensuring that all hardware and software is documented as received within 24 hours of receipt. Ensuring all new deliveries to be processed within 30 days of receipt at the warehouse.

Note: This position works in a warehouse setting, with some outdoor exposure during the workday. This role routinely uses standard office equipment such as computers, phones, document scanners, and photo copiers as well as standard warehouse equipment such as pallet jacks, hand trucks, box cutters and tape dispensers. The Contractor frequently is required to stand and walk. The contractor shall regularly lift and/or move objects up to 10 lbs and occasionally lift and/or move objects up to 50 lbs.

Tasks for Warehouse Manager Support:
The Contractor Shall

- Manage the receipt, checking in, storage and location of all incoming stock while meeting required completion targets.
- Enter all Receiving documents into the ECBC IT Warehouse database within 24 hours of receipt (or 1 business day). This requires Contractor to match Purchase Order (PO) numbers of received shipments with PO numbers of orders placed via the ECBC Acquisition Tracking Database.
- Ensure that each property item has been properly barcoded and recorded in the ECBC IT Warehouse Database after receipt.
- Provide a report of items received to the TPOC and the ECBC Acquisition Team, as requested.
- Coordinate with the ECBC Service Desk Imaging Team on the scheduling of all system imaging when required.

- Prepare Hand Receipt Form to be signed by the end user upon delivery of Property items. Ensure signed Hand Receipt Form is entered into the ECBC IT Warehouse database within 48 hours (2 business days) of Delivery.
- Prepare a Delivery Confirmation form to be signed by the end user upon delivery of Non-Property items. Ensure signed Delivery Confirmation Form is entered into the ECBC IT Warehouse database within 48 hours (2 business days) of Delivery.

- Prepare Return Merchandise Authorizations and prepare goods for shipment for any required product returns.
- Provide a report of items delivered to the TPOC and the ECBC Acquisition Team, as requested.
- Provide monthly Project/Status Reports to Service Desk Manager.
- Maintain standards of health, safety, hygiene, and security of the building as directed by the TPOC.
- Organize the warehouse and work area for orderliness at all times.
- Secure the ECBC Imaging Warehouse by ensuring that the warehouse is either occupied when open or locked when no personnel are present.
- Ensure appropriate disposal and/or recycling of trash.
- Communicate with other Team members, staff and customers via email, phone, and face-to-face discussion
- Brief the Team Leader and/or the TPOC on any issues or concerns.

3.13 WAREHOUSE TECHNICIAN

Personnel as a minimum shall have the following:

- Contractor personnel filling this position are to possess a DoD 8570.01-M baseline certification that satisfies the IAT II level prior to appointment.

- Within 6 months of appointment employee must obtain a Computing Eenvironment (CE) certification relevant to job duties, subject to discretion of organization Information Assurance Manager (IAM).

- Security Clearance level - Interim Secret is allowed until full Secret clearance is granted. Top Secret may be required on a case by case basis as determined by the TPOC.

Description of duties: The contractor shall effectively perform various central receiving warehouse and logistical functions, including receiving and/or delivering IT equipment. Contractor shall process appropriate delivery ticket documentation, load and move equipment; make deliveries and pick-ups for ECBC CIO. Contractor shall serve as a support for asset inventory. Contractor shall provide customer service to supported organizations and maintain appropriate documentation. Duties include the distribution and scheduling of all IT-related hardware and software that is purchased by the ECBC CIO Acquisition Team. Contractor must maintain 100% accountability of all products through the entire supply chain process. Contractor is responsible for coordination of the imaging of all hardware with the ECBC Service Desk Imaging Team. Contractor shall be responsible for scheduling all equipment deliveries and providing documentation to the Warehouse Manager for input into the ECBC IT Warehouse Database. ECBC requires all incoming hardware and software to be documented as received within 24 hours of receipt. ECBC also requires all new deliveries to be completed within 30 days of receipt at the warehouse.

Contractor shall support Windows Desktop, Laptop computers, printers and other standard equipment uninterrupted power supply (UPS), scanners, other IT peripherals associated with the user. The Contractor shall provide service center phone utilizing the Level II support technicians in accordance with DoD 8140.01.

Note: This position works in a warehouse setting, with some outdoor exposure during the workday. This role routinely uses standard office equipment such as computers, phones, document scanners, and photo copiers as well as standard warehouse equipment such as pallet jacks, hand trucks, box cutters and tape dispensers. The Contractor frequently is required to stand and walk. The contractor shall regularly lift and/or move objects up to 10 lbs and occasionally lift and/or move objects up to 50 lbs.

Tasks for Warehouse Technician Support:
The Contractor Shall

- Coordinate with the ECBC Service Desk Imaging Team on the scheduling of all system imaging when required.
- Provide Tier II of IT support through phone, remote assistance, and on-site service for all users.
- Update and maintain the current approved Microsoft Windows OS image and provide feedback, software, and configuration changes to the image team.
- Schedule delivery and pick-up appointments for each property item with the end user and return signed Hand Receipt Form to the Warehouse Manager.
- Schedule delivery and pick-up appointments for each non-property item with the end user and return the signed Delivery Confirmation Form to the Warehouse Manager.
- Ensure Delivery Tickets are entered into the Service Desk Ticketing System before delivery of items.
- Maintain standards of health, safety, hygiene, and security of the building.
- Secure the ECBC Imaging Warehouse by ensuring that the warehouse is either occupied when open or locked when no personnel are present.
- Ensure appropriate disposal and/or recycling of trash.
- Communicate with other Team members, staff and customers via email, phone, and face-to-face discussion

3.14 TRANSITION PLAN

TRANSITION-IN PLAN

There will be a transition period of between fifteen (15) and thirty (30) calendar days from date of contract award for the contractor to ramp up to meet all contractual requirements including a full complement of staff. Three days after task order award, the contractor shall submit a transition plan incorporating any suggestions the Government may have to best ensure a seamless transition-in.

TRANSITION-OUT PLAN

At the completion of this contract, the contractor shall support transition of all development products, artifacts, software and tools, which were funded under this contract, to the Government. A written plan shall be submitted by the contractor NLT ninety (90) days prior to the end of the task order, in accordance with delivery instructions provided by the Government. The transition-out plan shall be based on a maximum sixty (60) day period prior to the end of the task order. The Transition-Out Plan shall facilitate the accomplishment of a seamless transition from the incumbent to the incoming contractor/government personnel at the expiration of this Task Order. The Contractor shall identify transition activities, schedules and milestones for

turnover of work centers/functions and identify how it will coordinate with the incoming and or Government personnel to transfer knowledge regarding the following, as applicable:

a. Project management processes.
b. Points of contact.
c. Location of technical and project management documentation.
d. Status of ongoing technical initiatives.
e. Transition of personnel.
f. Establish and maintain effective communication with the incoming contractor/Government personnel for the period of the transition.
g. Inventory, inspection and transfer of IT software and hardware, licenses, and warranties.
h. Inventory, inspection and transfer of all contractor maintained classified data, equipment and devices, ensuring positive control, accountability, and chain of custody is maintained for all COMSEC sensitive items.
i. Technical artifacts and configuration baselines.
j. Elevated system privileges, IAW technical direction issued by the ECBC TPOC.
k. Operations, maintenance, helpdesk, engineering and logistics functions

3.15 GOVERNMENT DIRECTED OVERTIME/SURGE (OPTIONAL – THIS TASK IS A T&M CONTRACT TYPE):

It is anticipated that the Government may require the Contractor to work overtime or surge resources to support requirements under Section 3.0 of this Task Order. The contractor shall support these requirements, while continuing to provide standard contracted services. It should be noted that optional government directed overtime or surge may apply to any mandatory tasks under Section 3.0 of this Task Order.

For proposal purposes, the Not-to-Exceed (NTE) value of this option is $4,000,000.00 per year.

Typical examples of overtime support that could be exercised includes but is not limited to:

- Exercise support when adjusting the normal work schedule; minimizing/prohibiting leave of individual contractor employees; adjusting service performance requirements summary DOES NOT achieve the required coverage.
- IT Operations when adjusting the normal work schedule; minimizing/prohibiting leave of individual contractor employees; adjusting performance requirements summary DOES NOT achieve the required coverage.
- Crashing project schedule(s) to achieve Government directed completion dates.

Government directed overtime should only be used when all other possibilities have been exhausted. Overtime costs shall not be incurred unless authorized by the Contracting Officer (CO) or the Contracting Officer's Representative (COR) / TPOC and unless funding is available to cover incurred expenses.

At the time of exercising this optional support, at a minimum the Government shall

- Identify the event (exercise/operation/project) which is driving the overtime requirement
- Identify the specific services where overtime or surge is authorized
- Utilize the labor rates for that specific year (e.g. base year or OY1) and specific labor category
- Define level of effort expectations (i.e. 12-hour days, 6 days per week)
- Identify duration or end date when overtime is no longer required
- Provide an estimate on the number of overtime or surge hours required.

4.0 TASK ORDER DELIVERABLES AND REPORTS:

The Contractor shall provide documentation tailored to the requirement of the task order and/or the task orders issued under this task order. All days in proposed schedules are calendar days unless otherwise stated. Unless otherwise stated, each deliverable shall be provided to the TPOC. The Contractor shall be required to prepare and present briefings to the Government on the results of efforts undertaken by performance of the award. Government personnel will review the materials presented and evaluate them for accuracy and completeness. The Government will notify the Contractor of any edits, revisions, etc., required within five working days of receipt of deliverable. The Contractor shall be granted an additional five workdays after notification to provide those changes to the Government. The Contractor shall produce all documentation in accordance with DoD and ISO: 9000 documentation standards. The Contractor shall maintain version control and Configuration Management (CM) control of documents and store them in a document library accessible to the Government.

4.1 Task Order Deliverables Schedule

The table below summarizes the deliverables and reports required throughout the performance of work described in this PWS**.** Unless otherwise specified, electronic copies shall be delivered via email attachment. The format of specific deliverables shall be proposed by the contractor and agreed to by the Government.

PWS Reference	Deliverable	Frequency	Submission Procedure
3.1 Project Management Support	Standard Operating Procedures	Two Weeks After Task Order Award	Contractor Designated Format
	Post Award Service Level Performance Table	Initial, 30 days after award	Contractor Designated Format accessible via SharePoint site
	Proposed Changes to Service Level Measures and Metrics	Semi-annually	Contractor Designated Format
	Financial Reports	Monthly	Contractor Designated Format
	Written Recommendations for Implementation of Existing IT Policies	As requested by TPOC	Contractor Designated Format
	Quality Control Plan	30 Days After Task Award	Contractor Designated Format
	Risk Mitigation Reports	Monthly	Contractor Designated Format

	Project Progress Reports	Monthly	Contractor Designated Format
	Organizational Conflict of Interests (OCI) Mitigation Plan	60 Days After Task Award	Contractor Designated Format
3.2 System Administration Support	Written Test Plans for Planned Hardware/Software Implementations	Minimum of 1 Week Prior to Testing	Contractor Designated Format
	Written Testing Results of Hardware/Software Implementation Plan	Minimum of 1 Week Prior to Implementation	Contractor Designated Format
	Windows Server System Daily Logs	Within 24 Hours of Request by TCOC	Contractor Designated Format
	Systems Continuity of Operations (COOP) Plan	Two Weeks After Task Order Award	Contractor Designated Format
	After Action Reports	Within 48 hours of Corrective Action	Contractor Designated Format
	Significant Accomplishments Reports	Weekly	Contractor Designated Format
	SOPs	As Requested by TPOC	Contractor Designated Format
	Request for Change to Systems	Minimum of 1 Week Prior to Implementation	CCB Request for Change Online Form
3.3 Network Engineering/Operations Management Support	Network Continuity of Operations (COOP) Plan	Two Weeks After Task Order Award	Contractor Designated Format

	Information Briefs, White Papers, Written Recommendations on Network Vulnerabilities	Within 48 Hours of Findings	Contractor Designated Format
	Significant Accomplishments Reports	Weekly	Contractor Designated Format
	Project Updates	Monthly	Contractor Designated Format
	Network Map	30 Days after Task Order Award and as Requested by TPOC	Contractor Designated Format
	Requests for Change for Network Changes	Minimum 1 Week Prior to Implementation	CCB Request for Change Online Form
3.4 Cybersecurity – Support (Technical And Managerial)	Activity and Progress Report on Information System Audits	Weekly during System Audit Periods	Contractor Designated Format
	Risk Management Framework (RMF) Package for Information System	Within 90 Days of System Implementation	Format IAW DoD 8510.01
	Scorecard and Plan of Action and Milestones	Within 30 days of Security Control	Format IAW DoD 8510.01

	(POA&M) for Accreditation packages	Assessment	
	Vulnerability Incident Reports	Within 24 Hours of Breach	Format IAW AR 25-2
	Cyber Security Policy Documents	Within 1 week of New Policy Implementation	Contractor Designated Format
	Requests for Change for I/A Systems	Minimum 1 Week Prior to Implementation	CCB Request for Change Online Form
3.5 SharePoint Administrator	Disaster Recovery Plan (COOP) for SharePoint	Two weeks After Task order Award	Contractor Designated Format
	After Action Reports	Within 48 hours of Corrective Action	Contractor Designated Format
	Significant Accomplishments Reports	Weekly	Contractor Designated Format
	Requests for Change for SharePoint Systems	Minimum 1 Week Prior to Implementation	CCB Request for Change Online Form
3.6 Business Systems Analyst Support (Optional Position)	GFEBS Business Data Reports	As Requested by TPOC	Contractor Designated Format
	Functional Specifications Documents for New/Modified Systems	As Requested by TPOC	Contractor Designated Format

	Significant Accomplishments Reports	Weekly	Contractor Designated Format
	Systems Documentation Manuals	As Requested by TPOC	Contractor Designated Format
	Project Status Reports	As Requested by TPOC	Contractor Designated Format
3.7 SharePoint Solutions Architecture and Development Support	Concept of Operations and SOPs	As Requested by TPOC	Contractor Designated Format
	Customer Database Size Reports	Weekly	Contractor Designated Format
	Project Status Reports	Weekly	Contractor Designated Format
	After Action Reports	Within 48 hours of Corrective Action	Contractor Designated Format
	Software architecture, Design, and Development Documentation	As Requested by TPOC	Contractor Designated Format
	Site and Infrastructure Architecture Diagrams	As Requested by TPOC	Contractor Designated Format
	Team Foundation Server Reports	As Requested by TPOC	Contractor Designated Format

	Requests for Change to SharePoint Systems	Minimum 1 Week Prior to Implementation	CCB Request for Change Online Form
3.8 Privacy Officer (Optional Position)	Requests for Change to Privacy Policies	Minimum 1 Week Prior to Implementation	CCB Request for Change Online Form
	Privacy Policy and Procedure Documentation	As Requested by TPOC	Contractor Designated Format
	Privacy Impact Statements	As Requested by TPOC	Government Designated Format
3.9 IT Facilities Support	SOPs	2 Weeks After Awards of Task Order	Contractor Designated Format
	Instruction Manuals and User Guideline Documentation	As Requested by TPOC	Contractor Designated Format
	ITAS Waivers, Agreements and Acceptance of Clauses Documents, Justifications, Statements of Non-Availability	As Required	Government Designated Format
	Requests for Change to Acquisition and Mobile Device Policies and Systems	Minimum 1 Week Prior to Implementation	CCB Request for Change Online Form
3.10 Graphics Designer/Visual Information Support (Optional Position)	Print-Ready files for Print Specialist/Publication	As Requested by TPOC	Contractor Designated Format

3.11 Knowledge Management Support (Optional Position)	Metric, Success, and Use Case Reports	As Requested by TPOC	Contractor Designated Format
	Knowledge Management (KM) Status Reports	Monthly	Contractor Designated Format
	KM Program Progress vs. KM maturity Model Report	Semi-Annually	Contractor Designated Format
	KM Best Practices and Taxonomy Application to SharePoint Reports	Quarterly	Contractor Designated Format
	Revision of KM Strategy to Address Changing Future Needs	Annually	Contractor Designated Format
	KM SharePoint Site for Workforce Communication	Within 6 months After Task Order Award	Contractor Designated Format
3.12 Warehouse Manager	Report of Items Received	As Requested by TPOC	Contractor Designated Format
	Report of Items Delivered	As Requested by TPOC	Contractor Designated Format
	Status and Special Project Report	Monthly	Contractor Designated Format
	Property Receipt and Barcoding Documents	Upon Receipt of Items	Government Designated Format
	Hand Receipt and Delivery Confirmation Forms	As Requested by TPOC	Government Designated Format
	Return Merchandise Authorization Forms	As Requested by TPOC	Vendor Designated Format

	Significant Accomplishments Report	Daily	Contractor Designated Format
3.13 Warehouse Technician	Significant Accomplishments Report	Daily	Contractor Designated Format
	Equipment Delivery tickets	Upon delivery of items(s)	Government Designated Format
3.14 Transition Plans	Transition-In Plan	3 days After Task Award	Contractor Designated Format
	Transition-Out Plan	As Requested by TPOC	Contractor Designated Format
All	Trip Reports	Within 7 Working Days of Completion of Travel	Contractor Designated Format
12.0 Government Furnished Equipment (GFE)	GFE Inventory List	Annually	Contractor Designated Format

4.2 Deliverables Media

The contractor shall submit electronic deliverables in a format compatible with current versions of the specified software in use by the client, as follows:

1) Text Microsoft Word
2) Spreadsheets Microsoft Excel
3) Briefings Microsoft PowerPoint
4) Drawings Microsoft Visio
5) Schedules Microsoft Project
6) Interactive Performance Dashboard Sharepoint Site

Other file formats (example: .pdf) may be acceptable as mutually agreed and coordinated with the Government.

4.3 BASIS OF ACCEPTANCE

The basis for acceptance shall be compliance with the requirements set forth in the task order, the contractor's proposal and other terms and conditions of the task order. Deliverable items rejected shall be corrected in accordance with the criteria outlined below.

Deliverables will be inspected for content, completeness, accuracy and conformance to task order requirements. Inspection may include validation of information or software through the use of automated tools, testing or inspections of the deliverables.

4.4 General Acceptance Criteria

Deliverables will be accepted when all discrepancies, errors or other deficiencies identified in writing by the Government have been corrected. The general quality measures, set forth below, will be applied to each deliverable received from the contractor:

1) Accuracy – Deliverables shall be accurate in presentation, technical content, and adherence to accepted elements of style.
2) Clarity – Deliverables shall be clear and concise; engineering terms shall be used, as appropriate. All diagrams shall be easy to understand, legible, and relevant to the supporting narrative. All acronyms shall be clearly and fully specified upon first use.
3) Specifications Validity – All Deliverables must satisfy the requirements of the Government as specified herein.
4) File Editing – All text and diagrammatic files shall be editable by the Government.
5) Format – Deliverables shall follow Army guidance. Where none exists, the Contractor shall coordinate approval of format with the TPOC.
6) Timeliness – Deliverables shall be submitted on or before the due date specified.

For software development, the final acceptance of the software program will occur when all discrepancies, errors or other deficiencies identified in writing by the Government have been resolved, either through documentation updates, program correction or other mutually agreeable methods

4.5 Draft Deliverables

If the draft deliverable is adequate, the Government may accept the draft and provide comments for incorporation into the final version. All of the Government's comments to deliverables must either be incorporated in the succeeding version of the deliverable or the contractor must demonstrate to the Government's satisfaction why such comments should not be incorporated.

If the Government finds that a draft or final deliverable contains spelling/grammatical errors, improper format, or otherwise does not conform to the requirements, the document may be immediately rejected without further review and returned to the Contractor for correction and resubmission. If the contractor requires additional Government guidance to produce an acceptable draft, the contractor shall arrange a meeting with the TPOC.

4.6 Written Acceptance/Rejection by the Government

The Government will provide written acceptance, comments and/or change requests, if any, within fifteen (15) work days from Government receipt of the draft deliverable.

Upon receipt of the Government's comments the contractor shall have ten (10) work days to incorporate the Government's comments and/or change requests and to resubmit the deliverable in its final form.

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

4.7 Non-Conforming Products or Services

Non-conforming products not falling under the provisions of PWS section 4.6 ,shall be rejected. Deficiencies shall be corrected by the Contractor within ten (10) work days of the rejection notice. If the deficiencies cannot be corrected within ten (10) work days, the contractor shall immediately notify the COTR of the reason for the delay and provide a proposed corrective action plan within ten (10) work days.

5.0 TASK ORDER MANAGEMENT

Government Point of Contacts:

CLIENT REPRESENTATIVE / TECHNICAL POINT OF CONTACT (TPOC)

TECHNICAL POINT OF CONTACT (TPOC)

Mr. Shawn McElheny (Manage all tasks)
Bldg 5234 Fleming Road Gunpowder, MD 21010
Phone: 410-417-4749
Shawn.a.mcelheny.civ@mail.mil

Mr. John A. Carnahan (Manage all tasks)
ECBC CIO IT Program Manager/IMO/TCO
Phone: 410-436-9321
John.A.Carnahan3.civ@mail.mil

Mr. Jason Borchers (Tasks 3.4 and 3.8)
Edgewood Chemical Biological Center
Aberdeen Proving Ground (EA), Maryland
Phone: 410-436-6190
Jason.m.borchers.civ@mail.mil

Ms. Annie Legouri (Tasks 3.5, 3.6 and 3.7)
Edgewood Chemical Biological Center
Aberdeen Proving Ground (EA), Maryland
Phone: 410-417-2273
Annie.k.Legouri.civ@mail.mil

Mr. Paul Brozovic
Edgewood Chemical Biological Center
Aberdeen Proving Ground (EA), Maryland
Phone: 410-436-3340
Paul.g.brozovic.civ@mail.mil

CLIENT PROJECT LEAD(PL)
Mr. Shawn McElheny
Bldg 5234 Fleming Road Gunpowder, MD 21010
Phone: 410-417-4749
Shawn.a.mcelheny.civ@mail.mil

GSA CONTRACTING OFFICER
Alexander Garcia
GSA FAS, Mid-Atlantic Region
General Services Administration (GSA)
Federal Acquisition Service (FAS)
The Dow Building - 3rd Floor
100 S. Independence Mall West
Philadelphia, PA 19106
Office: 215-446-58XX
Email: Alexander.Garcia@gsa.gov

GSA CONTRACT SPECIALISTS
Thomas McCarthy
GSA FAS, Mid-Atlantic Region
General Services Administration (GSA)
Federal Acquisition Service (FAS)
The Dow Building - 3rd Floor
100 S. Independence Mall West
Philadelphia, PA 19106
Office: 215-446-58XX
Email:Thomas.McCarthy@gsa.gov

GSA PROJECT MANAGER/CONTRACTING OFFICER'S REPRESENTATIVE (COR)
Shail Shah
GSA FAS, Mid-Atlantic Region
General Services Administration (GSA)
Federal Acquisition Service (FAS)
The Dow Building - 3rd Floor
100 S. Independence Mall West
Philadelphia, PA 19106
Office: 215-446-5858
Email:Shail.Shah@gsa.gov

Michael Shepherd
GSA FAS, Mid-Atlantic Region
General Services Administration (GSA)
Federal Acquisition Service (FAS)
The Dow Building - 3rd Floor
100 S. Independence Mall West
Philadelphia, PA 19106
Office: 215-446-58XX

Email:Michael.Shepherd@gsa.gov

6.0 ORDER TYPE

This is a hybrid type of task order that will consist of Firm Fixed Price and Time and Material (only CLIN 3.17 shall be T&M) CLINs with line items for labor, travel and non-travel ODCs. It is anticipated that the FFP CLINs will be incrementally funded in accordance with DFARs clause 252.232-7007, "Limitation of Government's Obligation," included herein.

7.0 PERIOD OF PERFORMANCE

The base period of performance will be twelve (12) months from date of award/task order start date. There are four consecutive 12-month option periods to be exercised at the Government's discretion. These are anticipated dates.

1) Base Year: 20 May 2016 through 19 May 2017
2) Option Year 1: 20 May 2017 through 19 May 2018
3) Option Year 2: 20 May 2018 through 19 May 2019
4) Option Year 3: 20 May 2019 through 19 May 2020
5) Option Year 4: 20 May 2020 through 19 May 2021

8.0 PLACE OF PERFORMANCE

The place of performance is primarily at the Government's facilities. The contractor shall also support multiple sites (shown below) within the Continental United States (CONUS) throughout the task order's period of performance at the locations identified below.

Places of Performance:

- Edgewood Chemical Biological Center
- Dugway Proving Ground
- Army Materiel Systems Analysis Activity

9.0 HOURS OF OPERATION

ECBC CIO/RDECOM G-6 operational hours will be a 40 hour work week, with hours per day and days of the week being flexible to accommodate mission needs. The normal hours of operation are from 0730-1800 unless specified in individual task orders. Actual hours of operation may increase considerably for emergencies, unforeseen delays/problems, or increased customer workload. The Project Manager shall be responsible for coordinating emergencies or unforeseen problems with appropriate personnel to resolve any issues. The Project Manager, or designated alternate, shall be accessible (via text, phone, or e-mail) at all times and respond to emergencies within four hours. Set scheduled hours may be adjusted with fourteen days' notice to the Contractor to accommodate changes in the customer support environment and peak work periods. Any overtime shall be

approved in advance by the TPOC. Unless stated otherwise, contractor personnel shall work primarily on-site. Some tasks may be performed in part of or in full at other locations with prior approval of the Contacting Officer Representative (COR) or TPOC as requirements arise.

9.1 Telework
The contractor shall submit a request for approval to the TPOC prior to authorizing any contractor personnel to perform in a telework or remote manner outside of government or contractor facilities. Approval for telework or remote work will be provided on a case by case basis when justified in accordance with the current ECBC Policy.

9.2 Recognized Government Holidays - When a holiday occurs on a Saturday, Federal employees are normally granted the previous Friday as a holiday observance. When a holiday occurs on a Sunday, Federal employees are normally granted the following Monday as the holiday observance. The Federal government observes the following Federal holidays. If a Federal Holiday falls on a weekday, it is not recognized as a "business day". The Contractor shall not report for work on the below recognized Federal Holidays.

1) New Year's Day
2) Martin Luther King Jr. Birthday
3) Presidents Day
4) Memorial Day
5) Independence Day
6) Labor Day
7) Columbus Day
8) Veterans Day
9) Thanksgiving Day
10) Christmas Day

10.0 TRAVEL/OTHER DIRECT COSTS (ODCs)

10.1 TRAVEL
The Contractor shall be required to travel under this task order when determined necessary by the Government. Contractor personnel shall be required to travel to CONUS and/or OCONUS locations to meet requirements of supported organizations. The Contractor shall perform Temporary Duty (TDY) non-local travel, as required in the performance of this effort, as authorized by the TPOC. All required travel shall be approved by the TPOC prior to traveling. Contractor personnel's travel is solely the responsibility of the Contractor. Reimbursement for travel shall be performed in accordance with FAR 31.205-46 and the Joint Travel Regulation (JTR). The TPOC may change any scheduled travel by giving the Contractor five (5) days advance notice in writing provided the Contractor has not incurred any travel costs. Rates and clarification on travel issues can be found at the following website: http://perdiem.hqda.pentagon.mil/perdiem/. Only required travel previously approved by the TPOC will be reimbursed. Trip reports are required within seven working days of the completion of travel. Travel performed for personal convenience and daily travel to and from work at the Government or Contractor's facility shall not be reimbursed. Local Travel Mileage: the Contractor is authorized to charge the Government for local travel mileage using POV (based on current approved DoD travel regulation), not to exceed 50 miles per trip, anything outside APGEA will require TPOC approval.

The contractor shall submit an approved Travel Report to the TPOC within seven (7) days after returning from travel.

The following information shall be included in each Travel Report:

1) Name of traveler(s)
2) Purpose of the trip
3) Destination
4) Costs incurred
5) Dates traveled
6) Organizations/ persons contacted
7) Discussion of the results of the trip, including findings by unit and corrective action taken and/or needed

10.2 ODCS

The Government may require the contractor to purchase hardware, software, and related supplies critical and related to the services being acquired under the PWS. The Government may require training that is in scope with the requirements as stated in this PWS and shall be approved by the Government TPOC before any training is taken. Such requirements shall be identified at the time a Task Order is issued or may be identified during the course of the task order by the Government or the contractor.

At the discretion of the Government, the contractor shall transport equipment when determined necessary by the TPOC. The contractor shall be responsible for providing the vehicle(s) for all deliveries of equipment and touch labor/ticket remediation trips. The Contractor shall use a Contractor provided vehicle to transport and deliver the desktop and laptop computer systems to the end-user within the Aberdeen Proving Grounds – Edgewood Area (APGEA).

11.0 KEY PERSONNEL

To the maximum extent practicable, the contractor shall retain Key Personnel for at least the base period of performance.

The following shall be designated as Key Personnel:

PWS Section 3.1 - Project Manager
PWS Section 3.2 - Senior Administrator Team Lead
PWS Section 3.3 – Senior Network Team Lead
PWS Section 3.4 - Senior IA/Cyber Team Lead
PWS Section 3.7 - Senior Applications Development and Support Team Lead

In accordance with DFARS clause (52.237-9000 Key Personnel) the personnel listed above are considered essential to the work being performed hereunder. Prior to substituting, removing, replacing, or diverting any of the specified individuals, the Contractor shall notify the Contracting Officer 15 working days in advance and shall submit a written request and justification (including proposed substitutions) in sufficient detail to permit evaluation of the impact on this Contract. The proposed substitution of personnel must meet or exceed the education, experience, and other technical requirements of the personnel being replaced. No change in personnel shall be made by the Contractor without the prior written consent of the Contracting Officer. However, in urgent situations, as determined or agreed to by the Contracting Officer, an oral request to substitute key personnel may be approved and subsequently ratified by the Contracting Officer in writing. Such ratification shall constitute the

consent of the Contracting Officer required by this paragraph. The Contracting Officer will notify the Contractor within 10 working days after receipt of all required information of the decision on the substitution(s). In the event the proposed substitution of key personnel does not meet or exceed the education, experience, and other technical requirements of the personnel being replaced, the Government reserves the right to require continued performance of previously approved key personnel or to require substitution of acceptable replacements for the individuals specified below. The key personnel listed below may, with the consent of the contracting parties, be amended from time to time during the course of the Contract to either add or delete personnel as appropriate.

12.0 GOVERNMENT FURNISHED EQUIPMENT (GFE)

- The contractor shall have full access to GFE and software to perform the duties on the project while performing duties in government space. Government shall provide equipment, including both computer hardware and software, necessary for the contractor to perform the assigned work, unless otherwise specified, to fully satisfy all operational requirements of this contract. All Government Furnished Equipment referred to in this clause will remain the property of the Government and under the contractors' control at all times. The Contractor shall coordinate the request for, and the delivery of all GFE through the TPOC.

- The Government will provide the Contractor all existing GFE identified in the CDRL DD form 1423-2 List of Government Furnished Equipment (add figure) at task award.

- The Contractor shall maintain up-to-date records of all GFE by site. The Contractor shall conduct annual inventories of GFE or as requested by the TPOC, and provide the resulting list to the TPOC.

- The Contractor shall, at the end of the contract, return to the Government all equipment and property owned/or provided by the Government and subsequently delivered to or otherwise made available to the Contractor for use under the contract.

- The TPOC will approve the replacement of GFE/GFP due to normal wear and tear, if required. A joint assessment will be conducted by the Contractor and the Government to determine normal wear and tear. Repairs exceeding normal wear and tear will be the responsibility of the Contractor (e.g., damages to GFE/GFP due to negligence, lack of maintenance, or improper usage). Equipment will be evaluated annually and refreshed if the TPOC deems appropriate.

- The Contractor shall notify the TPOC <u>immediately</u> after the discovery of lost, damaged, or destroyed GFE/GFP. The Contractor shall investigate and submit a report of shortage, loss, damage, or destruction of GFE/GFP to the KO within two working days after the discovery. The Contractor shall report the specific property affected, including national stock number (NSN) or other identifying codes and nomenclature; the circumstances surrounding the loss, damage, or destruction; the estimated cost of alleviating the problem, if required; and the expected impact on provision of Contractor services, if any.

- The Contractor shall not remove GFE/GFP from the installation or other supported areas without written approval from the KO or designated Government representatives. DFARS 252.245-7002 "Reporting Loss of Government Property" provides additional guidance with respect to loss of Government property.

13.0 PERFORMANCE REQUIREMENT SUMMARY/QUALITY CONTROL PLAN (QCP)

In addition to the overall Post Award Service Level reporting as discussed in Paragraph 3.0, the Government intends to utilize a Quality Assurance Surveillance Plan (QASP) to monitor the quality of the Contractor's performance. The oversight provided for in the order and in the QASP will help to ensure that service levels reach and maintain the required levels throughout the contract term. Further, the QASP provides the COR with a proactive way to avoid unacceptable or deficient performance by individuals under the contract, and provides verifiable input for the required Past Performance Information Assessments. The QASP will be finalized immediately following award and a copy provided to the Contractor after award. The QASP is a living document and may be updated by the Government as necessary.

Customer support timeline – Standard baseline customer support is to be provided within 4 business hours of request. VIP support will be provided to GS 15 positions or higher will be provided within one business hour of request.

The Performance Metrics outlined below will be used to evaluate whether the contractor's performance is satisfactorily meeting the standards specified in the Performance Requirements Summary (PRS). While the table states that incentives may consist of positive past performance evaluations, it should be understood that failure to meet the performance metrics below will result in negative past performance evaluations.

Past performance evaluations will be submitted to the Contractor Performance Assessment Reporting System (CPARS) for all government agencies to review. Past performance evaluations will contain narratives explaining reasons for positive and negative evaluations.

The Contractor service requirements are summarized into performance objectives that relate directly to mission failure if not accomplished. The performance threshold briefly describes the minimum acceptable levels of service required for each requirement. These thresholds are critical to mission success.

Performance Objective	PWS Paragraph(s)	Performance Threshold	Surveillance Method
PRS #1 – Problem Summary Reporting	Deliver weekly after actual release in accordance with paragraph 3.1 of PWS	2% deviation from standard	Monitor
PRS #2 - Problem Resolution	Acknowledge reported problems within 8 hours of being reported. Resolve or elevate within 48 hours	2% deviation from standard	Monitor
PRS #3 –System Administration Support	Provide systems administrative support in accordance with paragraph 3.2 of PWS.	Meets all performance requirements 98% of the time. Surveillance is compiled monthly.	Observe, Monitor
PRS #4 – Network Engineering/Operations/ Management Support	Provide Network Engineering/Operations/Management in accordance with paragraph 3.3 of PWS	Meets all performance requirements 98% of the time. Surveillance is compiled monthly.	Observe, Monitor

PRS #5 –Information Assurance Support (Technical and Management)	Provide Information Assurance Management and Support in accordance with paragraph 3.4 of PWS	Meets all performance requirements 98% of the time. Surveillance is compiled monthly.	Observe, Monitor
PRS #6 –SharePoint Administrator	Provide SharePoint Administrator support in accordance with paragraph 3.5 of PWS	Meets all performance requirements 98% of the time. Surveillance is compiled monthly.	Observe, Monitor
PRS #7–Business Analyst Support	Provide Senior Business Analyst support in accordance with paragraph 3.6 of PWS	Meets all performance requirements 98% of the time. Surveillance is compiled monthly.	Observe, Monitor
PRS #8 –SharePoint Solutions Architecture and Development Support	Provide Senior SharePoint solutions architecture support in accordance with paragraph 3.7 of PWS.	Meets all performance requirements 98% of the time. Surveillance is compiled monthly.	Observe, Monitor
PRS #9 – Project Management Support	Provide Site Manager or Site Lead support in accordance with paragraph 3.1 of PWS.	Meets all performance requirements 98% of the time. Surveillance is compiled monthly.	Observe, Monitor
PRS #10 – Privacy Officer Support	Provide Privacy Officer Support in accordance with paragraph 3.8 of PWS.	Meets all performance requirements 98% of the time. Surveillance is compiled monthly.	Observe, Monitor
PRS #11– IT Facilities Support Specialist	Provide IT Facilities Support; support in accordance with paragraph 3.9 of PWS.	Meets all performance requirements 98% of the time. Surveillance is compiled monthly	Observe, Monitor
PRS #12 – Graphics Designer/Visual Information Support	Provide Graphics Designer/Visual Information Support in accordance with paragraph 3.10 of PWS.	Meets all performance requirements 98% of the time. Surveillance is compiled monthly	Observe, Monitor
PRS #13 – Knowledge Management Support	Provide Knowledge Management Support in accordance with paragraph 3.11 of PWS.	Meets all performance requirements 98% of the time. Surveillance is compiled monthly	Observe, Monitor
PRS #14 – Warehouse Management Support	Provide Warehouse Management Support in accordance with paragraph 3.12 of PWS.	Meets all performance requirements 98% of	Observe, Monitor, Inspect

		the time. Surveillance is compiled monthly	
PRS #15 – Warehouse Technician Support	Provide Warehouse Technician Support in accordance with paragraph 3.13 of PWS.	Meets all performance requirements 98% of the time. Surveillance is compiled monthly	Observe, Monitor, Inspect
PRS #16- Financial Statement Support	Begin at start of task order. Deliver 30 working days after actual release	Meets all performance requirements 98% of the time. Surveillance is compiled monthly	Inspect

The contractor shall develop and maintain an effective Quality Control Plan to ensure services are performed in accordance with this PWS. The Quality Control Plan (QCP) shall be submitted to the TPOC 30 days after contract award. The Government will provide written approval of the QCP. The QCP at a minimum shall meet the following:

- Structured to assure the individual responsible for Quality Control (QC) is independent from other parts of the Contractor's organization.
- Contain procedures for written and verbal communication with the TPOC or applicable PM regarding performance of the TO.
- Contain clear, measurable, and acceptable levels of performance to ensure that the performance standards established are met.
- Contain procedures for preventing defects and deficiencies, early detection of problems, and handling corrective actions without dependence upon Government intervention.
- Contain equipment operator maintenance related QC measures to ensure equipment is fully functional to the Original Equipment Manufacturer (OEM) standard for the equipment.
- Contain surveillance procedures for each service to be monitored under this PWS. These procedures shall identify the list of items under surveillance, who will perform the surveillance, the frequency and method of surveillance, and procedures for correction of deficiencies.
- Include a system to investigate and resolve customer complaints. The investigation results shall be documented within five days of receipt and forwarded to the TPOC to include immediate corrective actions to prevent future complaints.
- Provide a record of all Contractor QC checks and corrective actions. These files shall be maintained by the Contractor and shall be available upon request to the TPOC during the performance period.

14.0 SECURITY

The security requirements are defined in the attached DD Form 254 (Attachment XX) and will be in accordance with the AR 380-5, applicable security classification guide(s), guidance provided by the Government Point of Contact, and the NISPOM, DoD 5220 22-M.

Contractor personnel visiting any Government facility in conjunction with this contract shall be subject to the Standards of Conduct applicable to Government employees. Site-specific regulations regarding access to classified or sensitive materials, computer facility/IT network access, issue of security badges, etc., will be provided as required by the Government. All products, source code and scripts produced and their

associated work papers are to be considered the property of the Edgewood Chemical and Biological Center (ECBC). Work shall be performed in accordance with the DD254.

The Contractor shall be required to have a TOP SECRET Facility clearance (FCL). The Facility Security Officer (FSO) shall also have a Top Secret Clearance. Selected Contractor personnel fulfilling the requirements of the contract/task orders (see specific task sections above for the details of the security clearances required)and any exercised options are required to have up to a final TOP SECRET security clearance as directed by the TPOC prior to beginning work. All Contractor personnel shall read the National Industrial Security Program Operating Manual (NISPOM) and other applicable security regulations, which will be provided by the Technical Point of Contact (TPOC) or COR to Contractor personnel so they will familiarize themselves with the Government's IT regulations and policies. The Contractor FSOshall submit visit notifications via the Joint Personnel Adjudication System (JPAS) in the format prescribed by the ECBC CIO Security Manager. The provisions outlined above apply to Contractor and sub-contractors that may be employed during the course of this contract.

15.0 ANTI-TERRORISM (AT)

15.1 Antiterrorism (AT) Level I Training

All contractor and subcontractor employees requiring access to Army installations, facilities and controlled access areas shall complete AT Level I awareness training annually. Contractor personnel who have not completed this training within the past year shall take this training within 90 calendar days after task order 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 applicable contractor and subcontractor employee to the TPOC within 90 calendar days after completion of training. AT Level I awareness training is available at the following website: https://atlevel1.dtic.mil/at.

15.2 AT Awareness Training for Contractor Personnel Traveling OCONUS

This standard language requires US-based contractor employees and associated subcontractor employees make available and receive Government-provided AT awareness training specific to the Area of Responsibility (AOR) as directed by AR 525-13, Antiterrorism. The combatant commander directs specific AOR training content, with the unit Authority to Operate (ATO) the local point of contact (POC).

15.3 iWATCH Training

For those contractor or subcontractor employees with an area of performance within an Army-controlled facility, installation, or area, the contractor and all associated subcontractors shall brief all employees on the local iWATCH program (training standards provided by the requiring activity ATO). This locally-developed training informs employees of the types of behavior to watch for and instructs employees to report suspicious activity to the TPOC. This training shall be completed annually, and contractor personnel who have not completed this training within the past year shall take this training within 90 calendar days of task order award and within 90 calendar days of new employees commencing performance. The Contractor shall submit results to the TPOC no later than 120 calendar days after task award and within 120 calendar days of new employees commencing performance.

15.4 Access and General Protection/Security Policy and Procedures

For those contractor or subcontractor employees with an area of performance within an Army-controlled facility, installation, or area, the contractor and all associated subcontractor employees shall comply with applicable installation, facility and area commander installation/facility access and local security policies and procedures (provided by government representative). Also, the contractor shall provide all information required for background checks in accordance with installation access requirements accomplished by installation Provost Marshal Office, Director of Emergency Services or Security Office. The contractor workforce shall comply with all personal identity verification requirements as directed by Department of Defense (DoD), Headquarters, Department of the Army (HQDA), and/or local policy. Should the Force Protection Condition (FPCON) at any individual facility or installation change, the Government may require changes in contractor security matters or processes.

15.5 Contracts That Require Handling or Access to Classified Information

The contractor shall comply with FAR 52.204-2, Security Requirements. This clause addresses 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, notice of which was furnished to the contractor.

AT Level I Training: This provision/contract text is for Contractor employees with an area of performance within an Army controlled installation, facility or area. All Contractor employees, to include sub-contractor employees, requiring access to Army installations, facilities and controlled access areas shall complete AT Level I awareness training within sixty (60) 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 sub-contractor employee, to the TPOC. AT level I awareness training is available at the following website: https://atlevel1.dtic.mil/at.

Access and General Protection/Security Policy and Procedures: This standard language text is for Contractor employees with an area of performance within an Army controlled installation, facility or area. Contractor and all associated sub-contractors employees 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 Director of Emergency Services or Security Office. Contractor workforce shall 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.

iWATCH Training: This standard language is for Contractor employees with an area of performance within an Army controlled installation, facility or area. The Contractor and all associated sub-Contractors 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 TPOC. This training shall be completed within sixty (60) calendar days of contract award and within thirty (30) calendar days of new employees commencing performance with the results reported to the TPOC NLT thirty (30) calendar days after contract award or new employees commencing performance.

Contractor employees who require access to Government information systems: All Contractor employees with access to a Government information system shall be registered in the Army Training Certification Tracking System

(ATCTS) at commencement of services, and shall successfully complete the DOD Information Assurance Awareness prior to access to the information systems and then annually thereafter.

Contracts that require an OPSEC Standing Operating Procedure/Plan: The Contractor shall develop an OPSEC Standing Operating Procedure (SOP)/Plan within ninety calendar days of contract award. This SOP/Plan will be reviewed and approved by the responsible Government OPSEC officer, per AR 530-1, Operations Security. This SOP/Plan will include the Government's critical information, why it needs to be protected, where it is located, who is responsible for it, and how to protect it. In addition, the Contractor shall identify an individual who will be an OPSEC coordinator. The Contractor shall ensure this individual becomes OPSEC Level II certified, Per AR 530-1.

Contracts that Require OPSEC Training: Per AR 530-1, Operations Security, new Contractor employees shall complete Level I OPSEC training within thirty (30) calendar days of their reporting for duty. All Contractor employees shall complete annual OPSEC awareness training.

Information Assurance (IA)/Information Technology (IT) Training: All Contractor employees and associated sub-contractor employees shall complete the DoD IA awareness training before issuance of network access and annually thereafter. All Contractor employees working IA/IT functions shall comply with DoD and Army training requirements in DoD 8140.01, and AR 25-2 within six months of employment by the Contractor.

Information Assurance (IA)/Information Technology (IT) Certification: Per DoD 8140.01, 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 8140.01-shall be completed upon contract award.

Contracts That Require Handling or Access to Classified Information: The Contractor shall comply with FAR 52.204-2, Security Requirements. This clause involves access to information classified "Confidential," "Secret," or "Top Secret SCI" and requires Contractors to comply with 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, any notice of which has been furnished to the Contractor.

Information Assurance Contractor Training and Certification. Per DFAR Case 2006-D023, Contractor personnel accessing information systems must meet applicable training and certification requirements.

16.0 CONTRACTOR MANPOWER REPORTING

The requirements in this PWS shall be addressed in the Army Contractor Manpower Reporting System IAW DI IN XX. The Office of the Assistant Secretary of the Army (Manpower & Reserve Affairs) operates and maintains a secure Army data collection site where the contractor will report all contractor manpower (including subcontractor manpower) required for performance of this task order. The contractor is required to completely fill in all the information in the format using the following web address: **https://cmra.army.mil**. The required information includes:

1) Contracting Number
2) Fiscal Year (FY that the work was performed)
3) Order Number (Delivery Order, Task Order, or Purchase Order Number)
4) Requiring Activity Unit Identification Code
5) Command (Command of the Requiring Activity that would be performing the mission if not for the contractor)

6) Contractor Name
7) Total Invoiced Amount (the total dollars amount invoiced during the fiscal year, at the Task Order Level. This is the responsibility of the contractor.
8) Questions about Contract Performance (Contractors: Indicate if the order includes the above services)
9) Supporting directorate
10) Government Furnished Equipment
11) Contracting Officer (First Name, Last Name, Phone Number, and Email)
12) COR/TPOC (First Name, Last Name, Phone Number, and Email)
13) Contractor (First Name, Last Name, Phone Number, and Email)
14) Location Information (Federal Supply Code (FSC), City of Installation or Services, State, Zip and Country)
15) Direct Labor Hours
16) Direct Labor Dollars
17) Fund Cite

As part of its submission, the contractor shall provide the estimated total cost (if any) incurred to comply with this reporting requirement. The reporting period will be the period of performance not to exceed 12 months ending 30 September of each Government fiscal year and must be reported by 31 October of each calendar year. The contractor may use a direct XML data transfer to the database server or fill in the fields on the website. The SML direct transfer is a format for the transferring files from a contractor's system to the secure web 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.

17.0 ORGANIZATIONAL CONFLICT OF INTEREST (COI) AND NOD-DISCLOSURE AGREEMENT

The contractor agrees to accept and to complete all requirements identified in this PWS and not to contract with other Government contractors in such a way as to create an organizational conflict of interest. To avoid an organizational or financial conflict of interest and to avoid prejudicing the best interests of the Government, the task order may place restrictions on the Contractor, its affiliates, chief executives, directors, subsidiaries and subcontractors at any tier when placing orders. Such restrictions shall be consistent with FAR Part 9.505 and the clause entitled Organizational Conflict of Interest and shall be designed to avoid, neutralize, or mitigate OCIs that might otherwise exist in situations related to the requirement. Examples of situations which may require restrictions are provided at FAR Part 9.508.

All contractor personnel directly associated with this task order will be required to sign a non-disclosure statement that will be furnished at time of award. Non-disclosure statements, once signed, are to be furnished to the TPOC. Any conflict of interest or actions detrimental to the best interests of the Government may result in immediate termination for default.

18.0 SUBCONTRACTOR MANAGEMENT

The prime contractor shall be responsible for any subcontract management necessary to integrate work performed on this requirement and shall be responsible and accountable for subcontractor performance on this

requirement. The prime contractor will manage work distribution to ensure there are no Organizational Conflict of Interest (OCI) considerations. The addition of future subcontractors to the Prime contractor team after award must be justified and processed as required by the Government. Prior notification to the CO for approval is required.

19.0 RULES AND REGULATIONS:

19.1 The contractor shall as an independent contractor, and not as an agent of the Government.

19.2 The Contractor shall provide the necessary personnel, equipment, tools, materials, supervision and other items necessary for performance-based; non-personal service to perform the task outlined in the Performance Work Statement (PWS). The Contractor shall provide IT Technical and Staff Services Support/Cyber Security (CS) Support to the specific objectives of this PWS in Part 8. These services are to be performed primarily at the Aberdeen Proving Ground Edgewood Area, Edgewood Chemical Biological Center, Chief Information Office (ECBC CIO) location at building E5234 Fleming Road. The Contractor shall perform to the standards in this Performance Work Statement (PWS). It is designed to provide acceptable service levels or performance standards against which the Contractor's performance shall be measured.

19.3 No Contractor personnel performing sensitive duties shall be allowed to commence work on this effort until his or her trustworthiness has been favorably adjudicated/determined via a favorable National Agency Check (NAC). ECBC CIO/RDECOM G-6 retains the right to request removal of Contractor personnel, regardless of prior clearance or adjudication status, whose actions, while assigned to this task order, clearly conflict with the interest of the Government. The reason for removal shall be fully documented in writing by the TPOC and provided to the PM and the CO. If such removal occurs, the Contractor shall within five business days, assign qualified personnel to any vacancy or vacancies thus created. Performance of this task order may require the Contractor to access data and information proprietary to the Government agency or of such a nature that its dissemination or use, other than in performance of this task order, would be adverse to the interest of the Government or others. The Contractor shall not divulge information or release data developed or obtained in performance of this procurement action without prior written approval from the TPOC.

19.4 The Contractor shall be responsible for safeguarding all Government property provided for Contractor use. At the close of each work period, Government facilities, equipment, and materials shall be secured in a safe area pre-determined by the TPOC. The Contractor shall establish and implement methods of making sure all access credentials (Common Access Card (CAC); DD Form 1466, DoD Building Pass; issued to the Contractor employee by the Government are not lost or misplaced and are not used by unauthorized persons. No access credentials issued to the Contractor by the Government shall be duplicated. The Contractor shall develop procedures covering access credentials that shall be included in the Quality Control Plan. Such procedures shall include turn-in of any issued access credentials by Contractor personnel who no longer require access to Government information systems or Government facilities. The Contractor shall immediately report any occurrences of lost access credentials to the TPOC. In the event access credentials are lost or damaged, the Contractor employee shall immediately notify the TPOC who will notify the ECBC Security of the loss or damage and request re-issue of the credential. Multiple occurrences of loss or damaged access credentials will be reported to the CO. The Contractor shall prohibit the use of Government issued access credentials by any persons other than the Contractor employee to whom the

credential is issued. The Contractor shall prohibit the opening of secure or locked areas by Contractor employees to permit entrance of persons other than Contractor employees engaged in the performance of assigned work in those areas, or personnel authorized entrance by the ECBC Group Security Office.

19.5 Contractor and sub-contractor personnel performing work under this task order may inadvertently have access or assist in the development of proprietary information (e.g., cost or pricing information, budget information or analyses, specifications or work statements, etc.) or perform evaluation services which may create a current or subsequent Organizational Conflict of Interests (OCI) as defined in section 15 of this PWS.. The Contractor shall notify the CO immediately whenever it becomes aware that such access or participation may result in any actual or potential OCI and shall promptly submit a plan to the CO to avoid or mitigate any such OCI. The Contractor's mitigation plan will be determined to be acceptable solely at the discretion of the CO and in the event the CO unilaterally determines that any such OCI cannot be satisfactorily avoided or mitigated, the CO may affect other remedies as he or she deems necessary, including prohibiting the Contractor from participation in subsequent contracted requirements which may be affected by the OCI.

19.6 Contractor shall comply with DFARS 48 Code of Federal Regulations Part 252.204.7012, Safeguarding Unclassified Controlled Technical Information (UCTI) https://www.federalregister.gov/regulations/0750-AG47/safeguarding-unclassified-controlled-technical-information-dfars-case-2011-d039-)

19.7 The Contractor and their sub-contractors may be required to take Government directed training, to include annual computer users security training, information assurance and system administrator training, to support this effort as authorized and approved by the TPOC. The Contractor shall ensure that all personnel are in compliance with DoD 8140.01. On an annual basis, the contractor shall submit a proposed refresher-training plan to the TPOC for review and planning purposes.

19.8 The TPOC will approve and authorize in writing any training determined to be necessary. The Contractor shall provide their personnel with any training needed to obtain or maintain proper qualifications to perform under this task order; scheduling training so that it does not compromise performance. The Contractor shall also provide on-the-job training (OJT) for its personnel as directed by the Government, when the Government determines that an employee is not sufficiently qualified to perform under the task order. This OJT requirement shall be limited to obtaining only the skills needed for task order performance. Contractor personnel's training is solely the responsibility of the Contractor, unless otherwise directed by the TPOC. The Contractor shall maintain records of all scheduled and completed personnel training. The Contractor shall possess all required Government IT Certifications.

19.9 The Contractor shall develop a key Standard Operating Procedure (SOP) for the initial completion and ongoing maintenance of a DD5513-R Key Control Registry (pages 1 and 2) for the issuance of all keys/key cards during the period of performance of each task order. The SOP shall be submitted to the TPOC for review and approval within thirty days of task order award. The TPOC will provide approval within seven days of receipt. The Contractor shall ensure all keys/key cards issued to the Contractor are not used by unauthorized persons or duplicated. The Contractor shall prohibit the opening of locked areas by Contractor personnel to permit entrance of persons other than Contractor personnel engaged in the performance of assigned work in those areas, or personnel authorized entrance by the TPOC. The Contractor shall immediately report any occurrences of unauthorized use, lost, or duplication to the TPOC. The Contractor shall present the DD5513-R Key Control Registry, to TPOC, immediately upon request, at any time during the period of performance.

The Contractor shall develop a SOP for security control processes for the documentation of lock combination issuance and revocation. The SOP shall be submitted to the TPOC for review and approval within thirty days from task order award. The TPOC will provide approval within seven days of receipt. The documentation shall contain the full name of the personnel, the date of when the personnel were authorized knowledge of the lock combination, and from whom they were given the lock combination (to include the person's name, title, email address and work phone number). The Contractor shall ensure that the TPOC is notified immediately when personnel that have access to the lock combinations are no longer necessary. The Contractor shall ensure and document that personnel have been informed of their access being withdrawn. The Contractor shall present the Lock Combination log to the TPOC immediately upon request, at any time during the POP.

19.10 The contractor shall attend any post-award conference convened by the Contracting Activity in accordance with FAR Subpart 42.500. The Contracting Officer, COR, TPOC, and other Government personnel, as appropriate, may meet periodically with the contractor to review the contractor's performance. At these meetings the Contracting Officer will apprise the contractor of how the Government views the contractor's performance and the contractor shall apprise the Government of problems, if any, being experienced. The contractor shall also notify the Contracting Officer (in writing) of any work being performed, if any, that the contractor considers over and above the requirements of the task order. Appropriate action shall be taken to resolve outstanding issues. The contractor shall conduct monthly In-Progress Reviews (IPR) at a mutually agreeable time to be scheduled at award Kick-Off meeting. The contractor shall prepare and deliver a read-ahead document forty-eight (48) hours prior to the meeting and shall incorporate the following topics: agenda, task review, task schedule, action items, task past and future activities, issues, and a summary. The Contractor PM and designated employees shall participate with weekly/ monthly staff meetings as directed by the Government. Generally the agenda will consist of an executive summary and a description of the accomplishments, work-in-progress, planned work, and issues or problems relating to each task area. Also the PM shall ensure contractors submit a weekly accomplishment report for each task under this PWS task order to the TPOC and shall include CTE accomplishments, obstacles hindering accomplishments, work assignments, time lines, costs, expenditures, future plans, and personnel staffing matters. The Contractor shall consolidate the weekly accomplishments into the monthly reporting (due the 10th of each month).

19.11 All task order personnel attending meetings, answering Government telephones, corresponding by e-mail and working in other situations where their Contractor status is not obvious to third parties are required to identify themselves as such to avoid creating an impression in the minds of members of the public and other Government officials that they are Government officials. All documents or reports produced by Contractors shall be suitably marked as Contractor products and that Contractor participation is appropriately disclosed. Contractor personnel shall display their name and company name while in the Government work area, wear and display a building pass at all times while on a Government facility, and identify themselves as Contractor to include company name on all e-mail.

19.12 The contractor shall have full access to GFE and software to perform the duties on the project while performing duties in government space. Government shall provide equipment, including both computer hardware and software, necessary for the contractor to perform the assigned work, unless otherwise specified, to fully satisfy all operational requirements of this task order. All Government Furnished Equipment referred to in this clause will remain the property of the Government and under the contractors

control at all times. The Contractor shall coordinate the request for, and the delivery of all GFE through the TPOC.

20.0 CONTRACTOR PERSONNEL AND SPECIALIZED SKILLS:

The contractor to the best of their efforts shall ensure that their personnel, are qualified to perform their assigned tasks at the beginning of the period of performance. The Contractor is responsible for ensuring all contractor personnel and alternates possess and maintain appropriate current professional certifications during the execution of this task order. The candidates' specific qualifications should be clearly demonstrated and documented.

Contractor Staff Certifications - DoD 8140.01 shall require that all contractors who are (Systems Administrators – Sec 3.2) SA's are to have Security + certification. For Sections 3.3 3.4, 3.5, 3.6, 3.7, and 3.15, this task order requires DoD 8570.01 IAT II level Certification before being hired. In accordance with DoD 8140.01, a second certification called a CE (Computing Environment) is required within 6 months and needs to be associated with the type of equipment or software that the contractor works with on a daily basis. In order to achieve the highest possible standards there is a need to enhance the maturity of the management and delivery of IT services to ECBC.

If Contractor personnel depart the task order at the initiation of the Contractor, the Contractor shall provide twenty business days' notice and shall either have a replacement in place for a minimum of five business days prior to the incumbent's departure or provide the Government with the plan on maintaining appropriate Service Levels without replacing the individual. If a person departs on their own initiative, the Contractor shall notify the Government as soon as they become aware and shall either replace that person within five business days of the vacancy or provide the Government with the plan on maintaining appropriate Service Levels without replacing the individual. The Contractor shall be responsible for maintaining appropriate Service Levels whether replacement personnel are available or not. The Contractor shall efficiently manage the number of personnel supporting this task order to maximize efficiencies in work accomplishment under the PWS. The Contractor is responsible for ensuring all senior level employees possess and maintain current appropriate professional certifications during the execution of this task order. The Contractor shall not employ any person who is a threat to the health, safety, security, or general wellbeing of the Government, or any person who would create a conflict of interest or the appearance of a conflict of interest.

21.0 GOVERNMENT FACILITY SPACE AND EQUIPMENT:

The Government will provide space, furnishing, materials, supplies, and equipment not designated to be provided by the Contractor during the POP. General office equipment will be provided by the Government for the Contractor's use during the POP for each TO. General Office equipment consists of items such as; desk telephones, copiers, fax communications, computers, and connectivity with the Automatic Identification System (AIS) Land Area Network (LAN). These will be available at the Government site for the Contractor's use in performance, of the day-to-day work responsibilities. Telephone service is subject to the standard monitoring requirements of the Government telephone network. The Government-furnished phones are subject to security monitoring at all times. Use of these phones constitutes consent to security monitoring. The Contractor shall be responsible for all unofficial (non-Government) long distance calls. The Government intends to provide space in the Edgewood/Aberdeen area. The Contractor shall be responsible for treating all Government property and equipment as it is intended so that the property remains in good working condition and without damage. The

Contractor shall control all Government property assigned to them. The Contractor shall be required to sign a hand receipt for all equipment provided by the government.

21.1 All utilities available at the Government facility will be available for the Contractor's use in performance of duties outlined in this task order. The Contractor employees shall practice good conservation habits precluding the waste of utilities.

21.2 The work is typically be performing the required services in adequately lighted and climate-controlled areas. Government Furnished facilities may be equipped with building alarms to include security, fire, water and uninterruptable power sources. Contractor personnel shall cooperate in troubleshooting and reporting the cause of various alarms, in a manner commensurate with their assigned duties and shall respond to all evacuation and emergency egress procedures to preserve their safety.

21.3 Personally owned equipment shall not be connected to the Government network or utilized for processing or storing Government owned information. The Contractor shall give due consideration to tools the Government currently uses and for which possesses licenses to operate to capitalize on existing Government investments. If the Contractor identifies tools which will facilitate the successful accomplishment of this task order, the Contractor shall identify the item and provide a complete justification, with an estimated cost. The Government will make the final decision as to whether or not the tools are necessary to the efficient execution of the task order requirements. Anything furnished by the Government shall remain Government property. The Contractor shall provide all equipment required to maintain communications to meet the requirements of the task order (example, Blackberry and IPhone).

21.4 The Contractor shall provide a local off-site office and the necessary furniture and equipment, at the Contractor expense, to perform administrative and office functions.

22.0 UNSERVICABLE ITEMS

The Contractor shall provide assistance in providing disposition of unserviceable systems. This includes the proper handling and shipping of equipment requiring maintenance to the nearest warranty location or designated regional support center for repair in accordance with the system maintenance plan or turn-in to a local DRMO. The contractor shall maintain the necessary records for tracking and accountability purposes.

23.0 DATA RIGHTS

The Government and Contractor shall enter into an agreement with regards to Data Rights pursuant to FAR 25.227-11 and Far 25.227-13 and DFARS 252.227-7.13/ 252.227-7.14/ 252.227.7027. The Government requires unlimited rights to all documents/material and software produced under this Task Order. At a minimum all documents and materials, to include the source codes of any software produced under this task order, shall be provided with Government Purpose Rights. The Government shall have the right to use, modify, reproduce, release, perform, display or disclose technical data or computer software within the Government without restriction or outside the Government for U.S Government purposes. This right does not abrogate any other Government rights. All parties shall use electronic technologies to reduce paper copies of program information generated throughout the life of the task order and to communicate and pass data between government and contractor organizations.

24.0 INVOICES

The Period of Performance (PoP) for each invoice *shall* be for one calendar month. Monthly Firm Fixed Prices shall be in accordance with Section B of this Task Order. The contractor *shall* submit only one invoice per month per order/contract. The appropriate GSA office will receive the invoice by the twenty-fifth calendar day of the month after either:

1) The end of the invoiced month *(for services)* or

2) The end of the month in which the products *(commodities)* or deliverables (fixed-priced services) were delivered and accepted by the Government.

For Labor Hour and Time and Material orders/contracts each invoice shall show, the skill level category, the hours worked per skill level, the rate per skill level and the extended amount for that invoice period. It *shall* also show the total cumulative hours worked (inclusive of the current invoice period) per skill level, the hourly rate per skill level, the total cost per skill level, the total travel costs incurred and invoiced, and the total of any other costs incurred and invoiced, as well as the grand total of all costs incurred and invoiced.

For Labor Hour and Time and Material orders/contracts each invoice shall *clearly indicate* both the current invoice monthly "burn rate" and the total average monthly "burn rate".

The contractor shall submit all required documentation (unless exempted by the contract or order) as follows:

For Travel: Submit the traveler's name, dates of travel, location of travel, and dollar amount of travel.

For ODCs: Submit a description of the ODC, quantity, unit price and total price of each ODC.

Note: The Government reserves the right to audit, thus; the contractor shall keep on file all backup support documentation for travel and ODCs.

Note: For Firm Fixed Price, Labor Hour, and Time and Material fiscal task items:

Charges:

1) All invoice charges must be task item specific (only one task item) unless concurrent task item periods of performance exist.

2) For invoices with concurrent task item periods of performance all invoice charges must be service month specific (that is one service month only).

Credits:

1) If the credit invoice is for the same year of a particular ACT#, the contractor shall include that credit on a subsequent invoice submission against that same ACT#. If the contractor is unwilling to offset a subsequent invoice then they must submit a refund check.

2) When the credit invoice is for a different year, the contractor shall submit a refund check for that credit invoice.

Invoices that net to a credit balance **SHALL NOT** be accepted. Instead a refund check must be submitted by the contractor to GSA accordingly. The refund check shall cite the ACT Number and the period to which the credit pertains. The contractor shall provide the credit invoice as backup documentation. Do not attach credit invoice in ITSS or on the Finance website. It must be attached to the refund check. The refund check shall be mailed to:

General Services Administration
Finance Division
P.O. Box 71365
Philadelphia, PA 19176-1365

Posting Acceptance Documents: Invoices shall be submitted monthly through GSA's electronic Web-Based Order Processing System, currently ITSS to allow the client and GSA COTR to electronically accept and certify services received by the customer representative (CR). Included with the invoice will be all back-up documentation required such as, but not limited to, travel authorizations and training authorizations (including invoices for such).

Receiving Agency's Acceptance: The receiving agency has the following option in accepting and certifying services:

Electronically: The client agency may accept and certify services electronically via GSA's electronic Web-Based Order Processing System, currently ITSS, by accepting the Acceptance Document generated by the contractor. Electronic acceptance of the invoice by the CR is considered concurrence and acceptance of services.

Electronic acceptance of the invoice by the CR is considered concurrence and acceptance of services. The contractor shall seek acceptance and electronically post the acceptance document in GSA's electronic Web-based Order Processing System, currently ITSS. After acceptance of the invoice by the CR, the contractor shall submit a proper invoice to GSA Finance (*www.finance.gsa.gov/defaultexternal.asp*) not later than five (5) workdays after acceptance by the Government of the product, service, and/or cost item.

Note: The acceptance of the authorized agency customer representative is REQUIRED prior to the approval of payment for any invoiced submitted and shall be obtained prior to the approval of payment. In order to expedite payment, it is *strongly recommended* that the contractor continue to include the receiving agency's electronic acceptance of all the services or products delivered, with signature of the authorized agency customer representative and the date of acceptance, as part of the submission documentation.

Note: If *any* invoice is received without the required documentation and, the customer's electronic acceptance, the invoice *shall* be rejected in whole or in part as determined by the Government.

Posting Invoice Documents: Contractors shall submit invoices to GSA Finance for payment, after acceptance has been processed in GSA's electronic Web-Based Order Processing System, currently ITSS. The contractor is to post the invoice on GSA's Ft. Worth web site, *www.finance.gsa.gov/defaultexternal.asp*

The contractor is not authorized to add new skill level categories or vary between levels within the same labor category without approval of the Government, formalized in a signed modification by the Contracting Officer.

Content of Invoice: The contractor's invoice will be submitted monthly for work performed the prior month. The contractor may invoice only for the hours, travel and unique services ordered by GSA and actually used in direct support of the client representative's project. The invoice shall be submitted on official letterhead and shall include the following information at a minimum.

1) GSA Task Order Number
2) Task Order ACT Number
3) Remittance Address
4) Period of Performance for Billing Period
5) Point of Contact and Phone Number
6) Invoice Amount
7) Skill Level Name and Associated Skill Level Number
8) Actual Hours Worked During the Billing Period
9) Travel Itemized by Individual and Trip (if applicable)
10) Training Itemized by Individual and Purpose (if applicable)
11) Support Items Itemized by Specific Item and Amount (if applicable)

Final Invoice: Invoices for final payment must be so identified and submitted within 60 days from task completion and no further charges are to be billed. A copy of the written acceptance of task completion must be attached to final invoices. The Contractor shall request from GSA an extension for final invoices that may exceed the 60-day time frame.

The Government reserves the right to require certification by a GSA COTR before payment is processed, *if necessary*.

Close-out Procedures.

General: The contractor shall submit a final invoice within sixty (60) calendar days after the end of the Performance Period. After the final invoice has been paid the contractor shall furnish a completed and signed Release of Claims (GSA Form 1142) to the Contracting Officer. This release of claims is due within fifteen (15) calendar days of final payment.

25.0 CLAUSES

25.1 FAR 52.217-8 Option to Extend Services (NOV 1999)

The Government may require continued performance of any services within the limits and at the rates specified in the contract. These rates may be adjusted only as a result of revisions to prevailing labor rates provided by the Secretary of Labor. The option provision may be exercised more than once, but the total extension of performance hereunder shall not exceed 6 months. The Contracting Officer may exercise the option by written notice to the contractor within 30 days of the end of the task order period of performance.

(End of clause)

25.2 FAR 52.217-9 - Option to Extend the Term of the Contract (MAR 2000)

(a) The Government may extend the term of this contract by written notice to the Contractor within 30 days; provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least 45 days before the contract expires. The preliminary notice does not commit the Government to an extension.

(b) If the Government exercises this option, the extended contract shall be considered to include this option clause.

(c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed 66 months.

(End of clause)

25.3 FAR 52.237-3 Continuity of Services (JAN 1991)

(a) The Contractor recognizes that the services under this contract are vital to the Government and must be continued without interruption and that, upon contract expiration, a successor, either the Government or another contractor, may continue them. The Contractor agrees to—

(1) Furnish phase-in training; and

(2) Exercise its best efforts and cooperation to effect an orderly and efficient transition to a successor.

(b) The Contractor shall, upon the Contracting Officer's written notice, (1) furnish phase-in, phase-out services for up to 90 days after this contract expires and (2) negotiate in good faith a plan with a successor to determine the nature and extent of phase-in, phase-out services required. The plan shall specify a training program and a date for transferring responsibilities for each division of work described in the plan, and shall be subject to the Contracting Officer's approval. The Contractor shall provide sufficient experienced personnel during the phase-in, phase-out period to ensure that the services called for by this contract are maintained at the required level of proficiency.

(c) The Contractor shall allow as many personnel as practicable to remain on the job to help the successor maintain the continuity and consistency of the services required by this contract. The Contractor also shall disclose necessary personnel records and allow the successor to conduct on-site interviews with these employees. If selected employees are agreeable to the change, the Contractor shall release them at a mutually agreeable date and negotiate transfer of their earned fringe benefits to the successor.

(d) The Contractor shall be reimbursed for all reasonable phase-in, phase-out costs (i.e., costs incurred within the agreed period after contract expiration that result from phase-in, phase-out operations) and a fee (profit) not to exceed a pro rata portion of the fee (profit) under this contract.

(End of clause)

25.4 DFARS 252.232-7007 LIMITATION OF GOVERNMENT'S OBLIGATION (MAY 2006)

(a) Contract line item(s) *[Contracting Officer insert after negotiations]* is/are incrementally funded. For this/these item(s), the sum of $ *[Contracting Officer insert after negotiations]* of the total price is presently available for payment and allotted to this contract. An allotment schedule is set forth in paragraph (j) of this clause.

(b) For item(s) identified in paragraph (a) of this clause, the Contractor agrees to perform up to the point at which the total amount payable by the Government, including reimbursement in the event of termination of those item(s) for the Government's convenience, approximates the total amount currently allotted to the contract. The Contractor is not authorized to continue work on those item(s) beyond that point. The Government will not be obligated in any event to reimburse the Contractor in excess of the amount allotted to the contract for those item(s) regardless of anything to the contrary in the clause entitled "Termination for Convenience of the Government." As used in this clause, the total amount payable by the Government in the event of termination of applicable contract line item(s) for convenience includes costs, profit, and estimated termination settlement costs for those item(s).

(c) Notwithstanding the dates specified in the allotment schedule in paragraph (j) of this clause, the Contractor will notify the Contracting Officer in writing at least ninety days prior to the date when, in the Contractor's best judgment, the work will reach the point at which the total amount payable by the Government, including any cost for termination for convenience, will approximate 85 percent of the total amount then allotted to the contract for performance of the applicable item(s). The notification will state (1) the estimated date when that point will be reached and (2) an estimate of additional funding, if any, needed to continue performance of applicable line items up to the next scheduled date for allotment of funds identified in paragraph (j) of this clause, or to a mutually agreed upon substitute date. The notification will also advise the Contracting Officer of the estimated amount of additional funds that will be required for the timely performance of the item(s) funded pursuant to this clause, for a subsequent period as may be specified in the allotment schedule in paragraph (j) of this clause or otherwise agreed to by the parties. If after such notification additional funds are not allotted by the date identified in the Contractor's notification, or by an agreed substitute date, the Contracting Officer will terminate any item(s) for which additional funds have not been allotted, pursuant to the clause of this contract entitled "Termination for Convenience of the Government."

(d) When additional funds are allotted for continued performance of the contract line item(s) identified in paragraph (a) of this clause, the parties will agree as to the period of contract performance which will be covered by the funds. The provisions of paragraphs (b) through (d) of this clause will apply in like manner to the additional allotted funds and agreed substitute date, and the contract will be modified accordingly.

(e) If, solely by reason of failure of the Government to allot additional funds, by the dates indicated below,

in amounts sufficient for timely performance of the contract line item(s) identified in paragraph (a) of this clause, the Contractor incurs additional costs or is delayed in the performance of the work under this contract and if additional funds are allotted, an equitable adjustment will be made in the price or prices (including appropriate target, billing, and ceiling prices where applicable) of the item(s), or in the time of delivery, or both. Failure to agree to any such equitable adjustment hereunder will be a dispute concerning a question of fact within the meaning of the clause entitled "Disputes."

(f) The Government may at any time prior to termination allot additional funds for the performance of the contract line item(s) identified in paragraph (a) of this clause.

(g) The termination provisions of this clause do not limit the rights of the Government under the clause entitled "Default." The provisions of this clause are limited to the work and allotment of funds for the contract line item(s) set forth in paragraph (a) of this clause. This clause no longer applies once the contract is fully funded except with regard to the rights or obligations of the parties concerning equitable adjustments negotiated under paragraphs (d) and (e) of this clause.

(h) Nothing in this clause affects the right of the Government to terminate this contract pursuant to the clause of this contract entitled "Termination for Convenience of the Government."

(i) Nothing in this clause shall be construed as authorization of voluntary services whose acceptance is otherwise prohibited under 31 U.S.C. 1342.

(j) The parties contemplate that the Government will allot funds to this contract in accordance with the following schedule:

On execution of contract	$_____
(month) (day), (year)	$_____
(month) (day), (year)	$_____
(month) (day), (year)	$_____

(End of clause)

25.5 DFARS Clause 252.204-7012 SAFEGUARDING COVERED DEFENSE INFORMATION AND CYBER INCIDENT REPORTING (DEC 2015)

(a) *Definitions*. As used in this clause—

"Adequate security" means protective measures that are commensurate with the consequences and probability of loss, misuse, or unauthorized access to, or modification of information.

"Compromise" means disclosure of information to unauthorized persons, or a violation of the security policy of a system, in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object, or the copying of information to unauthorized media may have occurred.

"Contractor attributional/proprietary information" means information that identifies the contractor(s), whether directly or indirectly, by the grouping of information that can be traced back to the contractor(s)

(e.g., program description, facility locations), personally identifiable information, as well as trade secrets, commercial or financial information, or other commercially sensitive information that is not customarily shared outside of the company.

"Contractor information system" means an information system belonging to, or operated by or for, the Contractor.

"Controlled technical information" means technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. Controlled technical information would meet the criteria, if disseminated, for distribution statements B through F using the criteria set forth in DoD Instruction 5230.24, Distribution Statements on Technical Documents. The term does not include information that is lawfully publicly available without restrictions.

"Covered contractor information system" means an information system that is owned, or operated by or for, a contractor and that processes, stores, or transmits covered defense information.

"Covered defense information" means unclassified information that—

(i) Is—

(A) Provided to the contractor by or on behalf of DoD in connection with the performance of the contract; or

(B) Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract; and

(ii) Falls in any of the following categories:

(A) *Controlled technical information.*

(B) *Critical information (operations security)*. Specific facts identified through the Operations Security process about friendly intentions, capabilities, and activities vitally needed by adversaries for them to plan and act effectively so as to guarantee failure or unacceptable consequences for friendly mission accomplishment (part of Operations Security process).

(C) *Export control*. Unclassified information concerning certain items, commodities, technology, software, or other information whose export could reasonably be expected to adversely affect the United States national security and nonproliferation objectives. To include dual use items; items identified in export administration regulations, international traffic in arms regulations and munitions list; license applications; and sensitive nuclear technology information.

(D) Any other information, marked or otherwise identified in the contract, that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government wide policies (e.g., privacy, proprietary business information).

"Cyber incident" means actions taken through the use of computer networks that result in a compromise or an actual or potentially adverse effect on an information system and/or the information residing therein.

"Forensic analysis" means the practice of gathering, retaining, and analyzing computer-related data for investigative purposes in a manner that maintains the integrity of the data.

"Malicious software" means computer software or firmware intended to perform an unauthorized

process that will have adverse impact on the confidentiality, integrity, or availability of an information system. This definition includes a virus, worm, Trojan horse, or other code-based entity that infects a host, as well as spyware and some forms of adware.

"Media" means physical devices or writing surfaces including, but is not limited to, magnetic tapes, optical disks, magnetic disks, large-scale integration memory chips, and printouts onto which information is recorded, stored, or printed within an information system.

''Operationally critical support'' means supplies or services designated by the Government as critical for airlift, sealift, intermodal transportation services, or logistical support that is essential to the mobilization, deployment, or sustainment of the Armed Forces in a contingency operation.

"Rapid(ly) report(ing)" means within 72 hours of discovery of any cyber incident.

"Technical information" means technical data or computer software, as those terms are defined in the clause at DFARS 252.227-7013, Rights in Technical Data-Non Commercial Items, regardless of whether or not the clause is incorporated in this solicitation or contract. Examples of technical information include research and engineering data, engineering drawings, and associated lists, specifications, standards, process sheets, manuals, technical reports, technical orders, catalog-item identifications, data sets, studies and analyses and related information, and computer software executable code and source code.

(b) *Adequate security*. The Contractor shall provide adequate security for all covered defense information on all covered contractor information systems that support the performance of work under this contract. To provide adequate security, the Contractor shall—

(1) Implement information systems security protections on all covered contractor information systems including, at a minimum—

(i) For covered contractor information systems that are part of an Information Technology (IT) service or system operated on behalf of the Government—

(A) Cloud computing services shall be subject to the security requirements specified in the clause 252.239-7010, Cloud Computing Services, of this contract; and

(B) Any other such IT service or system (i.e., other than cloud computing) shall be subject to the security requirements specified elsewhere in this contract; or

(ii) For covered contractor information systems that are not part of an IT service or system operated on behalf of the Government and therefore are not subject to the security requirement specified at paragraph (b)(1)(i) of this clause—

(A) The security requirements in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations," http://dx.doi.org/10.6028/NIST.SP.800-171 that is in effect at the time the solicitation is issued or as authorized by the Contracting Officer, as soon as practical, but not later than December 31, 2017. The Contractor shall notify the DoD CIO, via email at osd.dibcsia@mail.mil, within 30 days of contract award, of any security requirements specified by NIST SP 800-171 not implemented at the time of contract award; or

(B) Alternative but equally effective security measures used to compensate for the inability to satisfy a particular requirement and achieve equivalent protection accepted in writing by an

authorized representative of the DoD CIO; and

(2) Apply other information systems security measures when the Contractor reasonably determines that information systems security measures, in addition to those identified in paragraph (b)(1) of this clause, may be required to provide adequate security in a dynamic environment based on an assessed risk or vulnerability.

(c) *Cyber incident reporting requirement.*

(1) When the Contractor discovers a cyber-incident that affects a covered contractor information system or the covered defense information residing therein, or that affects the contractor's ability to perform the requirements of the contract that are designated as operationally critical support, the Contractor shall—

(i) Conduct a review for evidence of compromise of covered defense information, including, but not limited to, identifying compromised computers, servers, specific data, and user accounts. This review shall also include analyzing covered contractor information system(s) that were part of the cyber incident, as well as other information systems on the Contractor's network(s), that may have been accessed as a result of the incident in order to identify compromised covered defense information, or that affect the Contractor's ability to provide operationally critical support; and

(ii) Rapidly report cyber incidents to DoD at http://dibnet.dod.mil.

(2) *Cyber incident report.* The cyber incident report shall be treated as information created by or for DoD and shall include, at a minimum, the required elements at http://dibnet.dod.mil.

(3) *Medium assurance certificate requirement*. In order to report cyber incidents in accordance with this clause, the Contractor or subcontractor shall have or acquire a DoD-approved medium assurance certificate to report cyber incidents. For information on obtaining a DoD-approved medium assurance certificate, see http://iase.disa.mil/pki/eca/Pages/index.aspx

(d) *Malicious software*. The Contractor or subcontractors that discover and isolate malicious software in connection with a reported cyber incident shall submit the malicious software in accordance with instructions provided by the Contracting Officer.

(e) *Media preservation and protection*. When a Contractor discovers a cyber incident has occurred, the Contractor shall preserve and protect images of all known affected information systems identified in paragraph (c)(1)(i) of this clause and all relevant monitoring/packet capture data for at least 90 days from the submission of the cyber incident report to allow DoD to request the media or decline interest.

(f) *Access to additional information or equipment necessary for forensic analysis*. Upon request by DoD, the Contractor shall provide DoD with access to additional information or equipment that is necessary to conduct a forensic analysis.

(g) *Cyber incident damage assessment activities*. If DoD elects to conduct a damage assessment, the Contracting Officer will request that the Contractor provide all of the damage assessment information gathered in accordance with paragraph (e) of this clause.

(h) *DoD safeguarding and use of contractor attributional/proprietary information*. The Government shall protect against the unauthorized use or release of information obtained from the contractor (or derived from information obtained from the contractor) under this clause that includes contractor

attributional/proprietary information, including such information submitted in accordance with paragraph (c). To the maximum extent practicable, the Contractor shall identify and mark attributional/proprietary information. In making an authorized release of such information, the Government will implement appropriate procedures to minimize the contractor attributional/proprietary information that is included in such authorized release, seeking to include only that information that is necessary for the authorized purpose(s) for which the information is being released.

(i) *Use and release of contractor attributional/proprietary information not created by or for DoD*. Information that is obtained from the contractor (or derived from information obtained from the contractor) under this clause that is not created by or for DoD is authorized to be released outside of DoD—

(1) To entities with missions that may be affected by such information;

(2) To entities that may be called upon to assist in the diagnosis, detection, or mitigation of cyber incidents;

(3) To Government entities that conduct counterintelligence or law enforcement investigations;

(4) For national security purposes, including cyber situational awareness and defense purposes (including with Defense Industrial Base (DIB) participants in the program at 32 CFR part 236); or

(5) To a support services contractor ("recipient") that is directly supporting Government activities under a contract that includes the clause at 252.204-7009, Limitations on the Use or Disclosure of Third-Party Contractor Reported Cyber Incident Information.

(j) *Use and release of contractor attributional/proprietary information created by or for DoD*. Information that is obtained from the contractor (or derived from information obtained from the contractor) under this clause that is created by or for DoD (including the information submitted pursuant to paragraph (c) of this clause) is authorized to be used and released outside of DoD for purposes and activities authorized by paragraph (i) of this clause, and for any other lawful Government purpose or activity, subject to all applicable statutory, regulatory, and policy based restrictions on the Government's use and release of such information.

(k) The Contractor shall conduct activities under this clause in accordance with applicable laws and regulations on the interception, monitoring, access, use, and disclosure of electronic communications and data.

(l) *Other safeguarding or reporting requirements*. The safeguarding and cyber incident reporting required by this clause in no way abrogates the Contractor's responsibility for other safeguarding or cyber incident reporting pertaining to its unclassified information systems as required by other applicable clauses of this contract, or as a result of other applicable U.S. Government statutory or regulatory requirements.

(m) *Subcontracts*. The Contractor shall—

(1) Include this clause, including this paragraph (m), in subcontracts, or similar contractual instruments, for operationally critical support, or for which subcontract performance will involve a covered contractor information system, including subcontracts for commercial items, without alteration, except to identify the parties; and

(2) When this clause is included in a subcontract, require subcontractors to rapidly report cyber incidents directly to DoD at http://dibnet.dod.mil and the prime Contractor. This includes providing the incident report number, automatically assigned by DoD, to the prime Contractor (or next higher-tier subcontractor) as soon as practicable.

(End of clause)

25.6 FAR 52.219-6 Notice of Total Small Business Set-Aside. (Nov 2011)

(a) Definition. "Small business concern," as used in this clause, means a concern, including its affiliates, that is independently owned and operated, not dominant in the field of operation in which it is bidding on Government contracts, and qualified as a small business under the size standards in this solicitation.

(b) Applicability. This clause applies only to—

(1) Contracts that have been totally set aside or reserved for small business concerns; and

(2) Orders set aside for small business concerns under multiple-award contracts as described in 8.405-5 and 16.505(b)(2)(i)(F).

(c) General.

(1) Offers are solicited only from small business concerns. Offers received from concerns that are not small business concerns shall be considered nonresponsive and will be rejected.

(2) Any award resulting from this solicitation will be made to a small business concern.

(d) Agreement. A small business concern submitting an offer in its own name shall furnish, in performing the contract, only end items manufactured or produced by small business concerns in the United States or its outlying areas. If this procurement is processed under simplified acquisition procedures and the total amount of this contract does not exceed $25,000, a small business concern may furnish the product of any domestic firm. This paragraph does not apply to construction or service contracts.

(End of clause)

25.7 FAR 52.219-14 Limitations on Subcontracting. (Nov 2011)

(a) This clause does not apply to the unrestricted portion of a partial set-aside.

(b) Applicability. This clause applies only to—

(1) Contracts that have been set aside or reserved for small business concerns or 8(a) concerns;

(2) Part or parts of a multiple-award contract that have been set aside for small business concerns or 8(a) concerns; and

(3) Orders set aside for small business or 8(a) concerns under multiple-award contracts as described in 8.405-5 and 16.505(b)(2)(i)(F).

(c) By submission of an offer and execution of a contract, the Offeror/Contractor agrees that in performance of the contract in the case of a contract for—

(1) Services (except construction). At least 50 percent of the cost of contract performance incurred for personnel shall be expended for employees of the concern.

(2) Supplies (other than procurement from a non-manufacturer of such supplies). The concern shall perform work for at least 50 percent of the cost of manufacturing the supplies, not including the cost of materials.

(3) General construction. The concern will perform at least 15 percent of the cost of the contract, not including the cost of materials, with its own employees.

(4) Construction by special trade contractors. The concern will perform at least 25 percent of the cost of the contract, not including the cost of materials, with its own employees.

(End of clause)