PROCUREMENT SENSITIVE

Communications and Information Technology Services (CITS III)

Task Order

Issued under the GSA Alliant 2 Government-wide Acquisition Contract (GWAC)

Issued By:

GSA Federal Acquisition Service
Mid-Atlantic Region
100 South Independence Mall West
Philadelphia, PA 19106

GSA ITSS ORDER NUMBER: ID03180060
DATE: 13 April 2022
AMENDMENT (VERSION): 23

SECTION C – PERFORMANCE WORK STATEMENT (PWS)

C.1. PURPOSE

The purpose of this Task Order is to provide communications and information technology (IT) services to support U.S. Africa Command (AFRICOM), U.S. European Command (EUCOM), Combined Joint Task Force - Horn of Africa (CJTF-HOA), and associated staff elements and organizations. All parties require devices, hardware, software, and network IT and communications support services for the continued enhancement, operation, maintenance, and life cycle support for networks, office automation, communications, and software and systems applications supporting C4 systems.

C.2. BACKGROUND

The stakeholder organizations supported under this Task Order are defined below. PWS Section C.2 and attachments appended to this PWS provide further information about the organizational and technical "footprints" covered under the scope as well as information about the Government oversight structure applicable to the administration and management of this Task Order. The intent of this task order is to provide services to support AFRICOM, EUCOM, CJTF-HOA, and associated staff elements and organizations. Due to the missions of these Combatant Commands (CCMDs) there is potential during the execution of this task order for one of the CCMDs to break-away from this task order into a separate contract/task order for the convenience of the Government. In the event that a decision is made to move forward with separate task orders, the Government will provide the Contractor notice of this intent along with an updated PWS to reflect the updated requirements. The scope of this requirement and the associated support services will remain the same.

C.2.1. ORGANIZATIONS

C.2.1.1. U.S. AFRICA COMMAND (AFRICOM)

HQ U.S. Africa Command (AFRICOM) is the geographic combatant command headquarters for the area of responsibility (AOR) covering Africa and the African Theater of Operations. It is currently headquartered at Kelley Barracks, Stuttgart, Germany.

The AFRICOM Command, Control, Communications and Computers Systems (C4) Directorate (ACJ6) currently provides theater-level policy, planning, and implementation oversight for C4 systems within the Areas of Responsibility (AOR). The ACJ6 provides the policy, plans, programs, and systems support to shape the C4 environment, ensuring information dominance, and interoperable C4 systems, to prevent conflict, respond in crisis, prepare for combat, and if required, fight to win.

C.2.1.2. U.S.EUROPEAN COMMAND (EUCOM)

HQ U.S. European Command (EUCOM) is the geographic combatant command headquarters for the AOR covering Europe and the European Theater of Operations.

The EUCOM Command, Control, Communications and Computers/Cyber (C4/Cyber) Directorate (ECJ6) currently provides theater-level policy, planning, and implementation oversight for C4 systems within the Areas of Responsibility (AOR). The ECJ6 provides the policy, plans, programs, and systems support to shape the C4 environment, ensuring information dominance, and interoperable C4 systems, to prevent conflict, respond in crisis, prepare for combat, and if required, fight to win.

C.2.1.3. COMBINED JOINT TASK FORCE – HORN OF AFRICA (CJTF-HOA)

The Combined Joint Task Force Horn of Africa is responsible for conducting operations and supporting AFRICOM directed activity across the Horn of Africa. CJTF-HOA, with Unified Action partners, develops and enhances influence, conducts military engagement and security force assistance in support of security cooperation, executes crisis response and contingency operations and sets the CJOA, in order to promote regional stability and protect US interests while maintaining operational access.
CJTF-HOA is located at Camp Lemonnier, Djibouti City, Djibouti and operates at contingency locations and forward operating locations across the Combined Joint Operating Area (CJOA).

The primary support contractor has responsibility to provide a full range of technology services to all end points that include front line help desk support, network, data, security, voice, VTC and video to users on Camp Lemonnier and at forward operating locations as well as interfacing with other Combatant Commands (CCMDs) and DoD communications environments.

C.2.1.4. U.S. ARMY AFRICA (USARAF)

U.S. Army Africa (USARAF), the Army Service Component Command (ASCC) for USAFRICOM, provides mission command, protects the force, sets the theater, conducts security force assistance, and supports joint and international partners in order to achieve AFRICOM and U.S. Army Campaign Plan objectives. Operating from Vicenza, Italy, USARAF conducts sustained security engagement with African land forces to promote security, stability, and peace.

USARAF G6 is responsible for the planning, coordination, employment, operation, and management of tactical and commercial communication systems and IT networks in support of USARAF's Area of Responsibility (AOR).

C.2.2. DOD ENTERPRISE SERVICE MANAGEMENT FRAMEWORK (DESMF)

IT Service Management provides a structured approach for managing the IT services. The contractor shall utilize the current version of the DoD Enterprise Service Management Framework (DESMF) and collaboratively identify areas where government interaction is required. The benefits of using IT Service Management (ITSM) are to provide a service delivery framework that:

- Gives continuity of services during and after task order transition.
- Promotes consistent delivery and management of Services to end users.
- Ensures CITS3 services are consistent with DoD CIO vision and policy.
- Remains focused on the delivery of services to end users.
- Responds to dynamic mission requirements and priorities.
- Implements new processes and improves current processes and functions.

The Government intends to achieve a fully developed ITSM model as outlined in the DESMF, and have it tailored to CCMD requirements. Table 5-1: DESMF Domains and Processes names the key DESMF ITSM domains and the specific processes associated with those domains. Table **Error! No text of specified style in document.**-2: DESMF Supporting Functions, identifies the support functions consisting of people who perform certain activities or types of work. The support functions manage the DESMF processes necessary to deliver effective and efficient IT services. Project management and governance are complementary to the DESMF. See Attachment A for reference to the full DESMF publication.

*Table **Error! No text of specified style in document.**-1: DESMF Domain's and Processes*

DESMF Domains	DESMF Processes
Service Strategy	Strategy Generation Management
	Business Relationship Management
	Demand Management
	Financial Management for IT
	Service Portfolio Management
	Service Catalog Management
Service Design	Design Coordination
	Availability Management
	Capacity Management
	Information Security Management
	IT Service Continuity Management
	Service Level Management
	Supplier Management
Service Transition	Transition Planning and Support
	Asset Management
	Change Management[1]
	Change Evaluation
	Configuration Management
	Knowledge Management
	Release and Deployment Management
	Service Validation and Testing
Service Operations	Access Management
	Event Management
	Incident Management
	Problem Management
	Request Fulfillment
Continual Service Improvement	CSI Metrics and Changes

[1] ITIL combines Asset and Configuration Management; therefore, the PWS reflects the newer ITIL change rather than the DESMF Process order.

Table **Error! No text of specified style in document.**-*2: DESMF Supporting Functions*

DESMF ITSM Supporting Functions
Engineering
Application Management
Technical Management
Service Desk
IT Operations Management

C.2.3. PROJECT MANAGEMENT BODY OF KNOWLEDGE (PMBOK)

The Project Management Services section uses a standards-based approach and relies upon guidelines, terminology, and definitions from a variety of commercial, government, and DoD sources on project management, particularly the Project Management Institute (PMI)-published PMBOK.

C.2.4. CAPABILITIES DELIVERED BY THE AFRICOM/EUCOM NETWORKS

The current AFRICOM and EUCOM networks have been deliberately implemented with a balance between technology and cost. Emerging technologies are actively monitored for potential incorporation into the existing architecture. As a result of careful technology consideration, the CCMDs have built and maintained stable, well-structured networks.

AFRICOM/EUCOM/CJTF-HOA requires the following capabilities for their networks:

- System Availability and Responsiveness
- IT Service Management
- Cybersecurity
- Data Protection
- Security
- Adaptability
- Collaboration
- Cross-Domain Security and Information Exchange
- System Interoperability
- Redundancy
- Survivability
- Scalability

The AFRICOM/EUCOM/CJTF-HOA Networks will serve as the Combatant Command's (CCMD's) instantiation of the DoD Information Network (DoDIN) and will use DoD-provided enterprise services to the greatest extent feasible. The AFRICOM/EUCOM/CJTF-HOA Networks need to minimize the transition impact between current DoD networks and the future vision for the DoD/CCMD Network Environment.

The AFRICOM/EUCOM/CJTF-HOA Networks will provide a set of core and enterprise applications and will serve as the CCMD's instantiation of an enterprise network to support unique applications.

AFRICOM/EUCOM/CJTF-HOA, along with DoD and Joint guidance, will define the methods in which future applications must be developed, and operate and establish rules for application hosting.

The AFRICOM/EUCOM/CJTF-HOA Networks will leverage the Net-Centric Core Enterprise Services (NCES) to the fullest extent possible, including Enterprise Services Management (ESM), Discovery & Delivery, Messaging, Collaboration, Mediation, Storage, Information Assurance (IA)/Security, Application, and User Assistant services. The AFRICOM/EUCOM/CJTF-HOA Networks will have common services criteria established that go across the Internet, NIPRNET, and SIPRNET environments to include a standard credentialing validation and directory. The AFRICOM/EUCOM/CJTF-HOA Networks will augment the DoDIN and NCES capabilities by guiding the transformation of the existing networks and legacy environments of applications, databases, networks, and facilities into an integrated enterprise information architecture capable of supporting Net-Centric Operations Warfare (NCOW). The AFRICOM/EUCOM Networks will provide terminal/seat, application, and data hosting services consistent with the common computing environment developed for DoD enterprise IT services.

The AFRICOM/EUCOM Networks will provide access to host-based applications as well as local client-server, web-based, and portal-based applications. The networks will provide access to network environments to include, but not limited to, Secure Internet Protocol Router Network (SIPRNET), Non-Secure Internet Protocol Router Network (NIPRNET), Multi-National Networks, Coalition Networks, and Internet consistent with DoD security guidelines. The certification and accreditation of these four environments has been completed. The AFRICOM/EUCOM Networks may be employed on a desktop alongside another hybrid client providing special functionality, including multi-level security.

Data hosting for joint supported applications will be provided through a mix of data centers structured to provide reliable, responsive access to data and information for the CCMD's warfighting and business communities. These data centers will provide application and data hosting as well as support application Continuity of Operations (COOP) requirements.

C.2.4.1. SYSTEM CAPABILITIES

Warfighters and business processes depend critically on assured and high quality communications, IT, and networking performance. The AFRICOM and EUCOM networks will support the warfighter and business communities by providing:

- Network services
- Communications services
- Video and presentation services
- Information Assurance/Cybersecurity
- Customer service and responsiveness
- Leveraging of DoD Enterprise services
- Domain architecture, engineering and installation
- Network Hardware services (i.e. Satellite/Antenna Maintenance)
- Governance

Note: The CJTF-HOA Network is an extension of the AFRICOM Network.

Challenges and risks the Government currently faces in delivering such capabilities to their customer base include:

- Responding to unforecasted change (i.e. Geo-Political events, change in network landscape)

- Addressing challenges that arise with routine operations
- Managing unknowns and emerging/changing requirements in light of uncertainties associated with the JIE initiatives
- Ensure real-time war-fighter support can be provided if there is a change in the EUCOM or AFRICOM AOR mission environment.

Communications and IT systems capabilities for AFRICOM/EUCOM/CJTF-HOA are best served by tiered requirements and associated threshold and objective criteria in terms of critical and non-critical services/capabilities.

C.2.4.2. SITES AND CUSTOMER BASE

Known sites and the customer bases supported under the Task Order's current footprint are listed below. Additional site(s) and number of personnel included in the user base is anticipated to grow during the period of performance of this Task Order. The current footprint includes:

- Kelley Barracks (Stuttgart, Germany) with approximately 50 EUCOM users and approximately 2500 AFRICOM users (4000 seats spanning SIPR/NIPR)
    - To include GO/FO/VIP Quarters. The AFRICOM VIP customer base consists of +/- 75 personnel GO/FO/Ambassadors/SES-level billets and their associated O-6 level staff.
- Patch Barracks (Stuttgart, Germany) with approximately 2700 EUCOM users (5400 workstations spanning SIPR/NIPR)
    - To include 20 General Officer (GO)/Flag Officer (FO)/Very Important Person (VIP) Quarters. The EUCOM VIP customer base consists of +/- 100 personnel GO/FO/Ambassadors/SES-level billets and their associated O-6 level staff.
- Camp Lemonnier (Djibouti City, Djibouti) with approximately 2500 AFRICOM users (4000 seats spanning SIPR/NIPR)
    - To include +/- 25 VIPs
    - To include support for CJTF-HOA Sites – both permanent and temporary as needed, which change from time to time, dependent on mission needs. Currently there are 7 supported Forward Operating Locations (FOLs) within the Combined Joint Operations Area (CJOA), though this number may expand or contract from time to time.
    - Contractor presence may be required at FOLs as required on a temporary basis.
- Stuttgart Army Airfield (Stuttgart, Germany) with approximately 150 AFRICOM users.
- Supreme Headquarters Allied Powers Europe (SHAPE) to include Chateau Quarters with approximately 200 EUCOM users in Mons, Belgium.
    - To include +/- 5 VIPs
- Pentagon with approximately 50 users (25 for each CCMD Liaison Office)
- RAF Molesworth, UK, with approximately 500 AFRICOM and 700 EUCOM remote users
- Office of Defense Cooperation (ODCs) and other remote locations in EUCOM's AOR countries, mostly in or near U.S. Embassies with approximate 41 remote sites. Each site has approximately 5-20 remote users, but varies between each site.
- George C. Marshall Center (Garmisch, Germany) with approximately 20 EUCOM remote users.
- Rome, Italy with approximately 10-15 remote AFRICOM users.
- Caserma Del Din (Vicenza, Italy) with approximately 1800 AFRICOM users
- Panzer Kaserne (Kaiserslautern, Germany) with approximately 20 remote AFRICOM users.

Note 1: Other potential future sites may occur in the EUCOM and AFRICOM AORs as needed.

Note 2: Very Important Person (VIP) - VIPs include end users in key leadership and management positions with enhanced service desk and desk side support service requirements. VIPs are located at the CCMD HQ as well as other sites supported under the scope of this Task Order

Note 3: Remote support indicates that a full-time on-site presence is not required at the time of award, but is subject to change in the future.

C.2.4.3. JOINT AND DOD-LEVEL CONSIDERATIONS

The AFRICOM/EUCOM/CJTF-HOA Networks will have common services criteria established that go across the NIPR and SIPR environments to include a standard credentialing validation service and utilization of the Identity and Access Management (IdAM) and Identity Synchronization Service (IdSS). The AFRICOM/EUCOM Networks will augment the DoDIN and Network Centric Enterprise Services (NCES) capabilities by guiding the transformation of the existing and legacy environments of applications, databases, networks, and facilities into integrated enterprise information architecture capable of supporting Net-Centric Operations and Warfare (NCOW). The AFRICOM/EUCOM Networks will also provide transport and high assurance guards, as required, for the approved networks that will initially remain separate (for example: Joint Worldwide Intelligence Communications System (JWICS), Combined Enterprise Regional Information Exchange System (CENTRIXS), Global Command Control System Joint (GCCS-J), Battlefield Information Collection and Exploitation System (BICES), etc.).

The AFRICOM/EUCOM/CJTF-HOA Networks Enterprise Services as a core capability of the AFRICOM/EUCOM/CJTF-HOA Network environments shall be the CCMD's instrument for the deployment of net-centric infrastructure and fielding of interoperable enterprise capabilities. These capabilities will mutually support and contribute to the Department of Defense (DoD) overall DoDIN Enterprise Services, NCES and IT capabilities. The AFRICOM/EUCOM/CJTF-HOA Networks shall deliver the enterprise IT infrastructure necessary for organizing and managing hardware, software and data as virtualized resources, hosting applications as services, using data sources, and offering NCES core services along with other core services as they become available. The infrastructure will support a Service Oriented Architecture (SOA) design methodology for connectivity between mission area processes and IT infrastructure using DoD and industry standard hardware and software building blocks. The overall intent of the AFRICOM/EUCOM Network Enterprise Services is to rationally transform the current infrastructure and management practices by implementing a disciplined enterprise approach to IT architecture, governance, and investment in concert with joint and DoD-level initiatives. This will improve the end-to-end process of how information is produced, organized, stored, protected, accessed, analyzed, collaborated, staffed, and presented to users.

C.2.5. CURRENT COMMUNICATIONS AND IT NETWORK ENVIRONMENT

AFRICOM/EUCOM/CJTF-HOA C4 systems include:

- Sensitive but Unclassified Wide Area Network (UWAN, also referred to as ULAN)
- Secret Wide/Local Area Network (SWAN, also referred to as SLAN)
- Commercial Service for Classified (CSfC)
- Coalition and Multi-National (to include bilateral) networks
- Unclassified Commercial Access Network (UCAN)
- Visual information, presentation and collaboration systems (desktop VTC systems, conference room VTC facilities)
- IPTV
- IP-based Telephony and wireless
- Conference and exercise facilities

- Customer service help desk

The AFRICOM/EUCOM/CJTF-HOA hardware infrastructure includes Intel-based PCs and Servers, UNIX servers, printers and other devices connected to the network (e.g., digital senders). The AFRICOM/EUCOM/CJTF-HOA Networks infrastructure includes fiber optic, coaxial, and twisted pair cabling. Network hardware includes components such as hubs, routers, and switches primarily from Cisco Networks. Operating Systems currently in use include Windows 2012/2016, and Oracle Solaris. The AFRICOM/EUCOM/CJTF-HOA C4 networks rely heavily on commercial-off-the-shelf (COTS) and Government-off-the-shelf (GOTS) software for most applications. Database management systems include: SYBASE, Oracle, and MS SQL. Office automation suites consist primarily of Microsoft Office.

See Attachments referenced in Section J for the full list of services, which depict the current configuration and status of networks covered under the TO's current footprint.

C.2.5.1. NIPRNET (ULAN/ UWAN)

The AFRICOM/EUCOM ULAN has wide-area connectivity to the Non-secure Internet Protocol Router Network (NIPRNET) and extends to remote sites to include, but not limited to, the Supreme Headquarters Allied Powers Europe (SHAPE) in Mons, Belgium, to the HQ EUCOM Liaison Office (ELO) and HQ AFRICOM Liaison Office (ALO) in the Pentagon, Washington, DC; JAC Molesworth, UK; ODC Sites; and to Camp Lemonnier, Djibouti (including CJTF-HOA FOLs).

The United States Army is the Executive Agent for AFRICOM/EUCOM, and provides the NIPRNET infrastructure to include connectivity over the Installation, Information and Integration Modernization Program (I3MP). The ULAN is connected to the Army's NIPRNET gateway. The Army (52d SSB) provides the NIPRNET circuit for the ULAN.

Note: ULAN/UWAN and NIPRNET terms are used interchangeably, but for the purposes of this requirement NIPRNET will be used. However, the ULAN terminology specifically refers to the AFRICOM/EUCOM portion of the unclassified network and is used to distinguish between the local portion of NIPRNET infrastructure used by AFRICOM/EUCOM and the external NIPRNET connectivity provided through 52d Strategic Signal Battalion.

C.2.5.2. SIPRNET (SLAN/SWAN)

The AFRICOM/EUCOM SLAN has wide-area connectivity to the Secure Internet Protocol Router Network (SIPRNET) and extends to remote sites to include, but not limited to, the Supreme Headquarters Allied Powers Europe (SHAPE) in Mons, Belgium, to the HQ EUCOM Liaison Office (ELO) and HQ AFRICOM Liaison Office (ALO) in the Pentagon, Washington, DC; JAC Molesworth, UK; ODC Sites; and to Camp Lemonnier, Djibouti (including CJTF-HOA FOLs).

Defense Information Systems Agency (DISA) directly provides the SIPRNET service for the SLAN. SLAN network is propagated through a secure distribution system and runs out to distribution points in the buildings. It then routes to each end user at AFRICOM/EUCOM. Any workspace that does not have access to the distribution points uses Inline Encryption Devices (INE) over their unclassified circuits.

The AFRICOM/EUCOM Networks SLAN will use the Gigabit or greater connectivity to the fullest extent possible. At a minimum, physically redundant capability will be provided while funding and fielding are pursued to provide the required diverse routing. Multi-Protocol Label Switching (MPLS) VPN COI

architecture can be used over the DoDIN when the capability is available to provide the AFRICOM/EUCOM Network logical separation from the NIPRNET/SIPRNET.

Note: SLAN/SWAN and SIPRNET terms are used interchangeably, but for the purposes of this requirement, SIPRNET will be used. However, SLAN terminology specifically refers to the AFRICOM/EUCOM portion of the secure network and is used to distinguish between the local portion of SIPRNET infrastructure used by AFRICOM/EUCOM and the external SIPRNET connectivity provided by DISA.

C.2.5.3. COMMERCIAL SOLUTION FOR CLASSIFIED (CSfC) GREY NETWORK

EUCOM has implemented a Commercial Solution for Classified network named FLAGSHIP in accordance with and approved for use by NSA. FLAGSHIP is a "grey" network which utilizes a layered architecture of Commercial Off-The-Shelf (COTS) equipment and public domain algorithms which satisfies the Information Assurance controls that are mandated for providing transport of classified networks. CSfC uses Capability Packages (CP) which contains product-neutral information that allows customers to build their solution based upon their specific needs. FLAGSHIP has implemented the Multi-Site Connectivity CP, Data At Rest (DAR) CP, and Mobility CP.

FLAGSHIP provides transport services for access to the EUCOM SLAN domain to approximately 50 endpoint devices/users. In its current configuration it could support approximately 200 consecutive sessions or endpoint devices. Endpoint devices may consist of laptops, tablets, or home kits (for use in VIP quarters). Primary users are EUCOM VIPs however the customer base extends beyond EUCOM personnel to include US Military personnel in Europe (i.e. AFRICOM, NATO, SOCEUR, SOCAFRICA, USAFE, USAREUR, etc.).

Future Considerations: Expand FLAGSHIP to provide transport for additional EUCOM managed domains such as CENTRIXS, SEAGULL, and/or US BICES. Additionally, EUCOM is exploring the possibility of providing FLAGSHIP as a transport service for other non-EUCOM managed domains such as AFRICOM, SOCEUR, and USAREUR. Implementing either of these considerations would require expanding the Grey Network by providing enclave-level services such as Active Directory, HBSS, automated scanning, etc. and additional support services would be considered when the need is identified.

C.2.5.4. COALITION AND MULTI-DOMAIN (TO INCLUDE BI-LATERAL) NETWORKS

AFRICOM/EUCOM has responsibility for the operations and maintenance of C4 coalition systems. Joint war-fighting operations demand responsive information exchange across combined forces and unified commands for planning, unity of effort, decision superiority, and decisive global operations. Coalition systems and networks are a combination of global, regional, local, multilateral and bilateral, virtually separate networks supporting multinational efforts. Coalition and bi-lateral local area networks/wide area networks (LAN/WAN) currently include ~~Combined Enterprise Regional Information Exchange System (CENTRIXS) SWA and~~ SEAGULL; limited support (primarily desktop) is provided to AMNET, MPE, BICES, CENTRIX GCTF, and CENTRIX CMNT.

AFRICOM/EUCOM is responsible for the operation of existing coalition network systems as well as the integration, migration, and acceptance of new systems and capabilities into the existing architecture. AFRICOM/EUCOM has responsibility for all aspects of support surrounding these networks and systems: system administration, security, certification and accreditation user account management, hardware maintenance, configuration management, software licensing, training, and other forms of user support.

C.2.5.5. UNCLASSIFIED CAMPUS AREA NETWORK (UCAN)

The Unclassified Campus Area Network (UCAN, aka Dirty Internet) provides AFRICOM/EUCOM users with a computing environment to process unclassified information. Access to the internet is provided by a commercial internet provider for AFRICOM and by DISA for EUCOM. UCAN is designed with minimal restrictions on users' access to the commercial Internet.

C.2.5.6. FUTURE CONSIDERATIONS

While the Local Area and Wide Area networks must be accredited to connect to the Defense Information Systems Network (DISN), future considerations should include the following:

- The AFRICOM/EUCOM/CJTF-HOA Networks will implement the Department of Defense's (DoD) net-centric enterprise services and data strategy where possible to further their goals in trying to reach a true joint net-centric enterprise solution.
- The AFRICOM/EUCOM/CJTF-HOA next generation enterprise networks will support net-centric operations for the larger Joint Network Environment.
- The AFRICOM/EUCOM/CJTF-HOA Networks will be a key enabler for the war fighter and business operations of the combatant commands and will provide net-centric capability that improves the enterprise IT services currently provided.

In the future, the network responsibilities under this Task Order could also extend to other locations in the AFRICOM and EUCOM AORs and the requirements for the number of nodes/locations supported could grow or change, dependent on mission needs of the Government and partner nations. At present, there is a potential for additional sites; however the expansion of coalition networks to other locations, including other sites within the AFRICOM and EUCOM AOR could be identified for inclusion during performance. Such work could entail: performance of site surveys to support deployment of coalition networks; supporting AFRICOM and EUCOM coalition CSSP/IA requirements; providing coalition network end user support; coalition network support; service desk and general operations and maintenance support. The Contractor would be expected to scale support up or down during performance as mission needs demand.

Key initiatives include the CCMDs' movement to the Joint Information Environment (JIE) under the Joint Regional Security Stack (JRSS). The JIE and JRSS are regional initiatives between 2nd Theater Signal Brigade (2TSB), Army Cyber Command (ARCYBER), Network Enterprise Technology Command (NETCOM), Regional Cyber Center – Europe (RCC-E), Defense Information Systems Agency (DISA), AFRICOM, and EUCOM to consolidate IT infrastructures within the European Theater. JIE is a DoD-level effort designed to collapse and consolidate the way IT services are provided across the DoD. The initiative looks at improving DoD's cyber posture through standardizing information assurance configurations; consolidating Service Component IT infrastructures into a common joint capability; streamlining network operations under a single joint construct; and providing a common IT governance structure for all of DoD.

As part of the initiative, the contractor shall be able to adapt to changes in the AFRICOM/EUCOM environment and be able to work in a mixed IT environment consisting of Active Duty, Government Civilians, and other Contractor personnel. Under the JIE, NIPRNET and SIPRNET have already migrated to enterprise email. Near future service areas to migrate could include Storage and Portal. In pursuit of DoD's desire for standardization, IT service consolidation, efficiencies and economies of scale, future changes may include providing support under the scope of this Task Order to other DoD organizations in the context of JIE.

C.3. SCOPE

The scope of this task order includes Communications and Information Technology (IT) services for AFRICOM and EUCOM networks; which include NIPRNET, SIPRNET, Multi-National Networks, Coalition Networks, and Commercial Internet consistent with DoD security guidelines. These services consist of the requisite labor to perform the technical, cybersecurity, program management, administrative, documentation, and reporting services detailed in Section C; the Other Direct Costs and Travel as defined in the logistical support annexes, and Tools necessary and ancillary to performance. Optional Services are to be invoked as a unilateral right of the Government.

The scope of the requirements detailed in Section C.5 provides for the full lifecycle of operations and maintenance of communications and IT services. The scope of such services described in this task order fall within the purpose of appropriations for Operations and Maintenance (e.g., sustainment, operation, and maintenance activities, as well as investment items below the $250,000 threshold) and as such it is anticipated that most requirements will conform to the definition of work properly charged as expenses under O&M appropriations. Although the routine activities under this task order are O&M in nature, the Government may encounter requirements under the scope of this task order where other appropriations types (e.g., Procurement or Research, Development, Test, and Evaluation (RDT&E) funding) may be required. It is recognized that per DoD 7000.14-R, Department of Defense Financial Management Regulation (DoD FMR), Volume 2A, Chapter 1, reference 010212 - Budgeting for Information Technology and Automated Information Systems, item B:

> *"The correct appropriation for budgeting an IT effort is dependent on the activity and the underlying tasks that make up the IT effort….An IT effort may require funding for more than one appropriation. The underlying purpose for each discrete task within an IT effort determines the correct appropriation for budgeting of that task. An effort that is so broadly defined that it contains separate tasks appropriate to budgeting in different appropriations should be separated into discrete tasks, each of which is budgeted in the correct appropriation."*

If appropriations other than O&M (such as Procurement or RDT&E) are required in the performance of this task order, the funding and work requirements shall be segregated, invoiced, tracked, managed and reported on separate line items to ensure work is charged to the proper appropriations consistent with DoD FMR requirements to segregate appropriations of different types. The guidelines provided within DoD FMR Volume 2A, Chapter 1, 010212 shall be utilized to determine which appropriation to use for a given requirement. The terms and definitions in the FMR and the criteria in Volume 2A, Chapter 1, item D "Procedures for Determining Expenses Versus Investments" shall be used to distinguish types of costs classified as an expense from those classified as investments.

C.4. OBJECTIVES

The objectives of this Task Order are to provide communications and IT services and procure state-of-the-art industry communications and information technology assets. The Government seeks an Industry partner that can:

- Provide flexible and scalable IT services that will enhance each supported activity's ability to respond to dynamic needs in their respective areas of responsibility.
- Deliver operational, technical, and program efficiencies to drive down costs without compromising the timeliness or quality of services.
- Optimize use of tools, technologies, bandwidth, capacity, and computing power in a manner that controls and reduces costs.

- Provide a best-of-breed approach and meld industry best practices with each supported activity functional expertise to develop optimal solutions to current and future command challenges.
- Manage workload surges effectively and in a manner that, given mission requirements and competing priorities, efficiently schedules and applies resources to meet the needs of supported activities without one activity's needs being given primacy over the other.

C.5. REQUIRED TASKS

C.5.1. GENERAL REQUIREMENTS

C.5.1.1. STAFF

The Contractor shall provide the requisite number of technically qualified personnel with appropriate security clearances, Information Assurance Technical (IAT), Information Assurance Management (IAM), and Computing Environment (CE) certifications to perform the communications and information technology tasks for the European and African theaters.

Note: See Section H for security clearance and IA certification requirements.

C.5.1.2. REGULATIONS, DIRECTIVES, AND STANDARDS

The Contractor shall follow Government regulations, directives, and standards while applying industry best practices and standards to the maximum extent possible. Contractor personnel shall have an understanding of these best practices, regulations, directives, and standards as appropriate for their specialized areas. The Contractor shall perform the work on this Task Order in accordance with (IAW) the guidance listed in Attachment A – Specific Governing Directives and IAW other documentation referenced elsewhere in this Task Order. This guidance is updated periodically over the period of performance and the Contractor shall perform the work on this Task Order IAW the latest updates.

C.5.1.3. 24 / 7 / 365 ON-SITE PRESENCE

CJTF-HOA and EUCOM requires their service desks to be staffed 24/7/365; therefore, no additional on-site presence is required. The contractor shall provide AFRICOM 24/7/365 on-site presence in Stuttgart, Germany (either on Patch Barracks or Kelley Barracks). The Contractor's designated point of contact must be able to triage the reported outage and contact on-call personnel when required. It is expected that the on-site POC will be able to perform normal duties as assigned.

C.5.1.4. ON-CALL SUPPORT

The Contractor shall provide on-call support for exceptional or emergency requirements which occur outside normal duty hours. Exceptional or emergency requirements are defined as all Priority 1 and 2 outages to include VIP end user devices

Note: See PWS Section C.5.1.6.3 for Priorities definitions

The Contractor shall establish procedures (to include on-call rosters) for each CCMD and CJTF-HOA (inclusive of FOLs as assigned) to be approved by each respective TPOC. The Contractor shall respond telephonically to an outage with a technician qualified in the required service area within:

- 1 hour of initial notification for all locations except CJTF-HOA.
- 30-minutes of initial notification for CJTF-HOA.

The Contractor shall respond on-site with a technician qualified in the required service area within:

- 2 hours of initial notification should the outage remain unresolved - for all primary locations except CJTF-HOA.
- 1 hour of initial notification should the outage remain unresolved - for CJTF-HOA.

On-site troubleshooting shall continue for as long as the outage remains unresolved.

Note: On-duty personnel may provide initial response; however, should the outage/problem remain unresolved they shall notify the on-call designated subject matter technician within the aforementioned time periods.

C.5.1.5. OPERATIONS AND EXERCISE SUPPORT

The Contractor shall participate in all operations and exercises, consistent with the level of service specified by the Government's technical direction. The scope of operations and exercise support includes, but is not limited to:

- Configuring and deploying hardware to support the operation/exercise
- Establishing new or expanding existing network services
- Establishing new or expanding existing Operation Centers
- Troubleshooting and resolving network and user problems

Requirements for providing operations/exercise support do not include providing support for Tactical Communications or Systems. Contractor support is limited to extending existing network services to the applicable remote sites as described in PWS Section C.2.4.2 or as identified by AFRICOM/EUCOM/CJTF-HOA. Travel may be required, and while these sites may be austere, the Contractor will not be required to deploy (travel) under field conditions.

The Contractor shall not increase manpower or man-hours for Operations or Exercise participation unless authorized by the Contracting Officer (CO) or the Contracting Officer's Representative (COR).

C.5.1.5.1. OPERATIONS SUPPORT

Operations are typically unannounced and have an unknown duration. The Contractor may be required to surge current work force to meet 24x7 operation needs. As much as possible this surge should be satisfied within existing staffing levels and without degradation of service. If needed the Contractor may request overtime and/or relief from service levels from the Government. Should operations continue long enough the Government may require or the Contractor may request additional resource be brought in TDY to meet mission needs.

C.5.1.5.2. EXERCISE SUPPORT

Exercises are planned events; therefore, although additional work may be required there should be sufficient time to schedule the work with minimal impact to current operations. The Contractor shall coordinate with the Government to adjust staff schedules to support exercises while concurrently delivering ongoing day-to-day services and support within the available staffing levels. Where directed by the Government, the Contractor shall provide 24x7 coverage during the exercises. This may include adjusting the normal work schedule or minimizing/prohibiting leave of individual contractor employees to achieve the required coverage. If needed the Contractor may request overtime and/or relief from service levels from the Government. The Contractor shall support the approximate number of exercises for each component below:

- AFRICOM: See Attachment C.8 – AFRICOM Exercise Support Data

- EUCOM: See Attachment D.16 – EUCOM Exercise Support Data

C.5.1.6. IT SERVICE MANAGEMENT (ITSM)

The Contractor shall provide and perform maintenance for all AFRICOM/EUCOM/CJTF-HOA *contractor supported equipment* communications and IT network systems, and devices, to include, but not limited to, the ULAN, SLAN, coalition, multi-national information systems, command and control, and other supported networks and systems, inclusive of:

- Windows-based, Oracle Solaris UNIX-based servers, and LINUX-based servers;
- Windows-based, Oracle Solaris UNIX-based, and MAC-based workstations, laptops, or tablets;
- Thin clients/zero client terminals;
- Printers and scanners connected to the AFRICOM/EUCOM/JTF-HOA networks;
- Video teleconferencing equipment;
- LAN hardware including hubs, routers, and switches;
- Connectivity devices from network drops to desktop; and
- End-user network-related telephony devices.

Note: Refer to Section J - Attachments for additional network, architecture, hardware/software and warranty information.

The Contractor shall ensure all supported hardware is repaired under warranty prior to issuing separate orders for repair, when possible. Should it become uneconomical to repair a piece of equipment, the TPOC will determine whether or not to fund the repair or the replacement of an item. The Contractor shall maintain spare and repair parts inventory and property accountability.

The Contractor shall develop and implement a standardized maintenance program for all contractor supported equipment as shown in the Supported Equipment List based on DoD guidance, industry standards or best practices, Original Equipment Manufacturer (OEM) service manuals, Service-based Technical Orders (TO) and established local procedures. The program shall include recurring preventive maintenance, and non-recurring Priority 1 – 3 maintenance to include: installation, removal, modification, troubleshooting, fault isolation, repair, replacement, reprogramming, or reconfiguration of equipment, systems, or networks. The program shall not include replacement or provisioning of consumables (e.g. paper, ink, or toner for printers).

C.5.1.6.1. CRITICAL SUCCESS FACTORS

Each of the CCMDs' operating networks will have their own defined scope: unique networks, unique service requirements, and unique user populations, which are further defined below (For example, EUCOM will require NIPR services, but only transport at some locations.). However, each operating network will be evaluated according to the below Critical Success Factors and Key Performance Indicators as identified in the Performance Requirements Summary. For the purposes of this PWS, listed below are the Service Category and Maintenance Priorities for ITSM.

C.5.1.6.2. SERVICE CATEGORIES

- Critical Services/Systems: Services or systems handling information that is determined to be vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of both content and timeliness. The consequences of loss of integrity or availability of these are unacceptable and could include the immediate and sustained loss of the CCMD's mission effectiveness.

- Essential Services/Systems: Services or systems handling information that is important to necessary for the conduct of day-to-day business, but does not materially affect support to deployed or contingency forces in the short-term. The consequences of loss of integrity are unacceptable and, while the loss of availability may be difficult to deal with, it can be tolerated for a short time. The consequences could include delay or degradation in providing important support services or commodities that may seriously impact mission effectiveness or operational readiness.
- Routine Services/Systems: Services, systems, or devices which may enhance operations or improve accessibility but are not absolutely necessary to conduct operations or day-to-day business in the short-term. The consequences of loss of integrity or availability can be tolerated or overcome without significant impacts.

C.5.1.6.3. MAINTENANCE PRIORITIES

Priority 1 is assigned to:

- Outages of all Critical Systems and Equipment
- Outages of Essential Systems and Equipment impacting more than 25% of users by CCMD
- Outages of designated VIP end user devices include office, home, and mobile locations
- Outages deemed critical by personnel authorized to give technical direction

Priority 2 is assigned to:

- Outages of all Essential Systems and Equipment not previously addressed in Priority 1
- Outages of End User Devices located in Mission Critical Areas (i.e. the Joint Operation Center) along
- Outages deemed serious by personnel authorized to give technical direction

Priority 3 is assigned to:

- Outages of all routine Systems and Equipment
- Outages of all other end user devices
- All scheduled maintenance outages

C.5.1.6.4. EVENT MANAGEMENT

The Contractor shall:

- Detect, prioritize, respond to, and log events affecting Service Operations or infrastructure.
- Log all events into CCMD authoritative ticketing system IAW CCMD Procedures.
- Notify Government of Priority 1 events or critical system disruptions, on-going resolution activities, and service restoration status IAW CCMD Policies and Procedures.
- Report the Event Management status summary IAW CCMD Policies and Procedures.

C.5.1.6.5. INCIDENT MANAGEMENT

The Contractor shall:

- Record, classify, prioritize, appropriately assign, resolve, and log Incidents. Incident resolution may include repairing, replacing, coordinating with vendors, or assumption of functionality by a redundant system.
- Report the incident status, including closure, to every customer.
- Notify Government of significant incidents, on-going resolution activities, and restored Service Operations IAW CCMD Policies and Procedures.

C.5.1.6.6. PROBLEM MANAGEMENT

The Contractor shall:

- Identify, monitor, and resolve underlying problems leading to incidents or events.
- Develop and deliver recommendations to the Government on enhancing performance and correcting problems.

C.5.1.6.7. REQUEST FULFILLMENT

The Contractor shall:

- Manage, control, and conduct the migration of people and assets through Installation, Move, Add, Change (IMAC) services. This includes hardware, software, configuration changes, equipment de-installation/relocation, data transfer, and user familiarization.
- Respond to other service requests to include hardware, software, configuration changes, equipment de-installation/relocation, data transfer, and user familiarization.
- Record, classify, prioritize, and assign the request to the proper response team.
- Deliver reliable connectivity, and end-user support services for communications and IT for designated residential network/systems access capability.
- Develop and deliver status and closure reports to appropriate stakeholders IAW CCMD Procedures.

C.5.1.6.8. CHANGE MANAGEMENT AND CHANGE EVALUATION

The Contractor shall:

- Record, classify, prioritize, and assign change requests IAW CCMD Procedures and governance boards.
- Resolve change requests IAW CCMD guidelines, directives, and governance boards.
- Report on summary status of change requests to include number of open and closed requests, length of open and open-to-close times.
- Execute a deliberate review of impact of proposed change requests to include use of test labs, as required, and identify costs, benefits, and risks to the Government for decision.

C.5.1.6.9. ADDITIONAL SPECIFIC TASKS

The Contractor shall:

- Develop and maintain a standardized Maintenance Management Plan. The Maintenance Management Plan shall include all processes,procedures, and key performance indicators (KPIs) used to implement the Contractor's standardized maintenance program.
- Incorporate available maintenance agreements and warranty contracts for parts and labor on supported equipment into their maintenance program.
- Schedule and perform maintenance that affects user services after core hours of operation, whenever possible, in order to minimize user impact.
- Coordinate and schedule outage requests for equipment maintenance IAW AFRICOM, EUCOM, and/or CJTF-HOA procedures governing this process.
- Notify the government before starting and upon completion of all Priority 1 or 2 maintenanace actions on operational equipment.
- Provide an estimated repair time to the designated Government representative within 1 hour after initial response for all Priority 1 & 2 maintenance actions.
- Provide updated status for all Priority 1 & 2 maintenance actions at intervals requested by the reporting activity, when it is known the estimated repair time will be exceeded, or upon repair/restoral, whichever is sooner.
- Document all maintenance actions into the government designated maintenance management system.
- Provide the Government a summary report of all maintenance actions to include preventive maintenance inspections and services.
- Provide Data Center/Communications Closet/Telecommunications Rooms (TRs) facility management support to include:
    - Monitoring Heating, Ventilation and Air-conditioning systems and power systems,
    - Notifying the Service Desk, Watch Officer and TPOC when established thresholds are exceeded,
    - Server and Network rack and cable management.

C.5.1.7. IT SERVICE CONTINUITY MANAGEMENT (ITSCM)

ITSCM consists of two distinct, yet interrelated parts – Disaster Recovery and Continuity of Operations. Disaster recovery is purely an IT function consisting of identifying, collecting, and storing the organizations data should a disaster occur. Continuity of Operations involves the whole organization and develops plans for what services are needed and how they would be provided should the need develop. As such it encompasses much more that IT services such as personnel, facilities, logistics support, etc. Often the Continuity of Operations Plan (COOP) will incorporate the Disaster Recovery Plan (DRP) in whole or in part.

C.5.1.7.1. DISASTER RECOVERY (DR)

The Contractor shall:

- Assess recovery strategies, processes and locations to develop the Disaster Recovery Plan for Government approval.
- Implement the plan to ensure identified data is available in case of a disaster.
- Participate in DR Exercises as directed by the Government; submit results and/or an after action report post exercise.

C.5.1.7.2. CONTINUITY OF OPERATIONS PLAN (COOP)

The Contractor shall:

- Assist the Government to develop the IT portion of the Continuity of Operations Plan to include assessing the viability of potential sites, designing the technical solutions, and developing the IT COOP strategy.
- When required and according to the plan, provide the required staffing to activate and operate the IT component at the Continuity of Operations site.
- Participate in COOP exercises:
    - Based on Government requirements, develop or assist in the development of exercise plans or scenarios to test the COOP.
    - Participate as direct In the COOP exercise.
    - Provide a written assessment or after action report post exercise.

C.5.2. COMMON REQUIRED TASKS

~~These enterprise level tasks are required by AFRICOM, EUCOM, and CJTF-HOA and may be provided as shared services, customer specific, or both (i.e. AFRICOM and EUCOM shared, CJTF-HOA stand-alone).~~
The Contractor shall provide analysis, administration, maintenance, and technical support for hardware, software, procedures, and peripheral equipment for the various networks, enclaves and systems that make up the AFRICOM, EUCOM, and CJTF-HOA information systems. These information systems shall provide services to a range of joint service end points that include data, voice, and video users; a mix of end-user accounts, and interfaces to other CCMD and DoD communications environments.

~~The following list of Services may be considered Shared between stakeholder organizations:~~

- ~~System Administration~~
- ~~System Security~~
- ~~System Storage Capacity Planning~~
- ~~COOP~~
- ~~Pentagon Support~~
- ~~Portal Services~~
- ~~Collaboration Services~~

- ~~Web Services~~
- ~~Multi-Factor Authentication (CyberArk)~~

Note: For the ~~initial~~ current task order ~~award~~ performance, only ~~these services and~~ TSCMIS (see paragraph C.5.2.2.27) may be shared. ~~Post award~~ In the future the contractor may propose or the Government may direct additional services to be shared between AFRICOM and associated service components, staff elements, and/or organizations.

C.5.2.1. END USER SUPPORT SERVICES

C.5.2.1.1. SERVICE DESK SUPPORT TECHNOLOGIES

The Contractor shall:

- Operate and manage remote access solution for troubleshooting.
- Operate and manage Ticketing System to support Incident Management, Security Incident Management, and Service Requests processes.

Note: The Contractor shall utilize the Ticketing System and Tools provided by the Government for each CCMD, unless otherwise directed by the COR and TPOC.

As the primary point of contact, the Service Desk is the interface between the user and the service. If there is an issue whether it is an unclear Event or Alert message, an Incident or Problem, or an Access issue, the user is going to contact the Service Desk for assistance if the issue cannot be resolved through self-help methods. The Contractor shall:

- Function as the CCMD Service Desk lead and the single interface between Government and external Service Providers and their respective Service Desks IAW CCMD Policies and Procedures.
- Follow CCMD Policies for Service Tickets that apply to externally managed systems.
- Operate and manage Service Desk capabilities (tools, processes, and reporting capability) on classified networks IAW CCMD Service Level Agreements. (core hours, 24/7/365 support)
- Report Service Desk metrics IAW CCMD Service Level Agreements.
- Notify government when escalation thresholds or service criticality thresholds are reached.
- Develop web-based mechanisms for users to initiate service desk requests.
- Develop, update, and maintain self-help for common problems and information requests via Frequently Asked Questions.
- Process Change Requests and forward to request fulfillment.
- Run the incident management process from incident recording to final incident closure.
- Deliver CCMD Walk-In Services as an interface to the Service Desk.
- Deliver building walk-through services to provide interfaces to the Service Desk.
- Operate and manage a remote access capability to assist in troubleshooting.

C.5.2.1.2. ACCOUNT MANAGEMENT

The Contractor shall provide a consolidated account management service desk which provisions and de-provisions IT systems accounts as personnel are assigned to or departing from the CCMD. The Account Service Desk shall be open during normal business hours (M-F, 0800-1700) except for US Holidays.

Assigned contractor staffs are required to certify and perform as Enhanced Trusted Agents (ETAs) for SIPR/Alt Token services. Account management services shall include as a minimum:

- Validation of 8570M requirements
- Account creation/deletion
- Updating of GAL information
- Issuance and management of User Agreements
- Multi-Factor Authentication Token services (issuance, reconstitution, PIN resets, revocations, out-processing)

The Contractor shall develop, deliver, and maintain a Service Operations Plan, including Processes found in Table 5-1, with review and approval by the Government, within 30 days of task order award, or as directed by the Government.

C.5.2.1.2.1. ACCESS MANAGEMENT

The Contractor shall provide services to authenticate identity (unique distinguishing information on an individual) and authorize access services and data (IdAM) to include:

- Create, modify, deactivate, and remove user and non-person entity (NPE) accounts (e.g. services, groups, distribution lists), as directed, IAW DoD policy, guidelines, and directives.
- Issuance, validation, and management of Government-directed account documentation IAW DoD and CCMD Policy. Examples include user agreements, DD2875, DD2140, and Training Certificates.
- Upon account deactivation, retain network end user data associated with an account IAW DoD Policy.
- Report Access Management status summaries to the Government IAW required reporting intervals.

The Contractor shall Certify and perform as Enhanced Trusted Agents (ETAs) for SIPR/Alt Token services; Synchronize data among Government provided user management databases and systems, to include Global Address Lists (GAL) with DISA's authoritative enterprise identify and contact attributes (IdSS); and Audit and report unauthorized personnel access discovered through IdAM program to the Government IAW DoD and CCMD Policy.

C.5.2.1.2.2. ENHANCED TRUSTED AGENT (ETA) SUPPORT SERVICES

The Contractor shall:

- Perform ETA services during normal work hours.
- Perform Local Registration Authority (LRA) services whenever LRA is not available.
- Offer walk-in and appointment-based services.
- Procure, print, issue, and revoke Tokens IAW DoD Policy.
- Troubleshoot Token failures to include PIN resets.
- Request certificates for new or reconstituted cards from the LRA.
- Revoking tokens when required.
- Train and certify sufficient staff to provide continuous service during normal core work hours.

C.5.2.1.2.3. MULTI-FACTOR AUTHENTICATION

The Contractor shall:

- Review, make recommendations for, and develop CCMD Policy and technical strategy for two-factor authentication.

- Integrate components of, transition, and operate two-factor authentication technical solutions IAW CCMD Policy and technical strategy (e.g. PKI).
- Integrate capabilities and features of the two-factor authentication technical solution, as directed.

Note: The current multi-factor authentication solution in place is CyberArk. Support for CyberArk is described in the Specialized Application Services Section.

C.5.2.1.3. DESKTOP DEVICES (VOIP, PC, LAPTOP, DVTC, PRINTER)

C.5.2.1.3.1. DESKTOP SUPPORT SERVICES

The Contractor shall provide desktop support services that include, but are not limited to:

- Connect end user IT and telephony devices; resolve any connections, software configuration, or hardware issues; and migrate data from replaced device to the new device.
- Deliver, unpack, remove packing materials, dispose of old equipment IAW CCMD Disposition procedures.
- Deliver end users the capability to self-install and configure software for which they are authorized.
- Problem recognition, research, isolation, resolution, tracking, and follow-up.
- Tier 2 support to end users for desktop, thin client, network, applications, or hardware.
- Coordinate and interact with the IT service provider.
- Recommend hardware, software, and modifications to meet end user requirements and/or mitigate issues.
- General touch labor support.
- Support for other technologies such as VTC Suite Operations.

The Contractor shall provide Tier 3 Customer Support Administrators (CSAs) to provide focalized technical services and end user customer support to a specific building or specialized group (customer base) of users. The purpose of this support is to provide more accessible support to a targeted part of the populace. The Contractor may be required to develop alternate work schedules for review and approval by the Government and provide support during work hours that fall outside of the normal duty hours. Some Contractor employees shall be dedicated to an assigned building and consider the building as their prime work location(s). The building locations and/or customer base where required dedicated CSA services are required is defined below:

AFRICOM	EUCOM	CJTF-HOA
Bldg 3314 Command Section	Bldg 2314	Bldg 300
AFRICOM Event Center	Bldg 2307 Roger's Conference Center	
Bldg 3317 JOC	Bldg 2358 JOC	
HQ AFRICOM Liaison Office (ALO)- Pentagon	HQ EUCOM Liaison Office (ELO)- Pentagon	

C.5.2.1.4. DATA TRANSFER AGENT (DTA) SERVICES

The Contractor shall:

- Perform DTA duties, as directed by CCMD Policy and Procedures. DTA Services shall perform DTA Services in bulk to the best of their ability.

- Manage the DTA program, including documentation and tracking of DTA actions IAW DoD Directives and CCMD Policy.
- Operate and manage tools and systems necessary to manage the DTA program.

C.5.2.1.5. LOANER LAPTOP SERVICES

The CCMDs require the ability to quickly issue loaner laptops to their personnel to support temporary, short-term engagements. Up to 100 laptops per CCMD may be required, and must have the ability to connect to one of several networks (e.g. NIPR, SIPR, bi or multi-lateral), specified at the time of request. This service is only to maintain the laptop library, issue laptops, and reconfigure upon return; once issued end-user assistance is the responsibility of the Enterprise Service Desk. The Contractor shall:

- Manage the Loaner Laptop program, which provides laptops to authorized remote or TDY users IAW CCMD Procedures, CCMD Remote Access policies, and Configuration Management baselines.
- Configure and issue laptops for CCMD-approved requests.
- Upon laptop return, configure laptop to serviceable status.
- Report activity summaries that include, at a minimum, the number of laptops issued that week and any delinquent users (overdue laptops).

C.5.2.1.6. VIP SUPPORT

The Contractor shall operate and manage specialized, Government-provided communications equipment kit within living quarters and specific campus office locations supporting personnel specified in CCMD Senior Leader Support List and VIP List. The Contractor shall provide configuration and maintenance for KLAS satellite terminals used by VIPs while travelling. Examples of kit technology includes end user computing devices, networking, voice, wireless, cryptologic, video, satellite, and messaging technology.

The Contractor shall prioritize response in periods of high support requests IAW CCMD Procedures and designated SLAs. If none exits, the Contractor shall recommend a proposed support prioritization schedule to Government for approval.

The contractor shall provide core hours support to living quarters and specific campus office locations and augment with 24/7/365 on-call support.

C.5.2.1.7. CONFERENCE CENTER SUPPORT

The Contractor shall manage Conference Center IT operations. Services shall be limited to user-facing IT functions. Example tasks include setting up IT services prior to conferences, aiding guests in accessing and operating IT systems, ensuring IT systems are operational, initial troubleshooting of IT systems, and assisting external technicians when troubleshooting. Locations include: AFRICOM Event Center, AFRICOM Office of Shared Services, AFRICOM Command Conference Center, and EUCOM Rogers Conference Center.

C.5.2.1.8. REMOTE SUPPORT SERVICES

The Contractor shall provide connectivity and IT end-user support services for Permanent Remote Sites and Temporary Sites to include:

- Sites that are not physically co-located with the core command network
- Supporting multiple users at the remote site (as opposed to individual quarters connectivity)
- Sites that are intended to remain in the same location for an extended period of time, usually on the order of years.

- Sites that are designated as a Forward Operating Location (FOL)

The Contractor shall:

- Upon Government direction, travel to enduring, remote and contingency locations to provide, manage, and operate IT services, for example, Email, shared file storage, network printing, domain name service, internet protocol address management, account management, token reset (limited to primary support locations), cyber security, and COMSEC.
- Manage the transport of equipment via Government-approved channels, including packing, shipping, unpacking, installation, and configuration, disposal of packing materials, and disposal/destruction of equipment, when directed. Examples of equipment include workstations, servers, network devices, cabling, smart phones, printers, telephony, and VTC systems.
- Configure all systems IAW current architectures and applicable DoD and CCMD Policies.
- Perform hardware and software maintenance and troubleshooting, as required.

C.5.2.2. ENABLING SERVICES

C.5.2.2.1. EMAIL SERVICES

The Contractor shall:

- Deliver, operate, and manage end-user Email clients.
- Deliver, operate, and manage end-user Email classification marking tools.
- Manage the integration of DoD email as a CCMD service to process, deliver, store, and receive email and associated attachments to end-user devices.
- Submit requests to email service provider to enable new email accounts, remove accounts, and troubleshoot email services and modify distribution lists.
- Manage distribution list IAW CCMD Procedures.
- Upon direction and applied only to specified networks, deliver full email services.
    - Deliver, operate, and manage back-end email infrastructure including email servers, as directed.
    - Email services include the ability to send and receive email with attachments with mission partners on the respective networks.
    - Archive and retain user mailbox data IAW DoD and CCMD Policies and Procedures.

C.5.2.2.2. CHAT/INSTANT MESSAGING SERVER

The Contractor shall:

- Deliver, operate, and manage end-user Chat/Instant Messaging clients.
- Manage the integration of chat messaging to process, deliver, and receive chat IAW current architectures.
- Manage chat groups and accounts IAW CCMD Procedures.
- Deliver, operate, and manage Chat/Instant Messaging Servers and supporting infrastructure, as directed.

C.5.2.2.3. IMAGE SERVICES

The Contractor shall:

- Maintain baseline images, update capabilities based on user requirements, ensure compliance with security requirements in accordance with cyber policies, test, implement, and manage CCMD images IAW Configuration Management and Release Management processes.
- Update images upon release of the vendor updates or directed compliance orders. Include the cumulative security and quality updates with those updates and all other updates released since the last image update.

C.5.2.2.4. PRINT SERVICES

The Contractor shall:

- Deliver, operate, and manage print services.
- Configure authenticated print release at each printer, as directed.
- Repair, or replace inoperative printers and dispose of all printers, if unable to restore to service.

C.5.2.2.5. KNOWLEDGE MANAGEMENT (KM)

C.5.2.2.5.1. AFRICOM KNOWLEDGE MANAGEMENT (KM)

The Contractor shall:

- Establish/integrate technical solutions or approaches that support the CCMD Knowledge Management program in fostering discovery, access, and sharing of organizational information and business processes, as directed.
- Perform KM operation, sustainment, maintenance, deployment, training, and change management of the knowledge management software, systems, and networks.
- Develop and deliver policy, governance, and process recommendations that improve knowledge management.
- Recommend use of Government- and Commercial Off-The-Shelf (GOTS/COTS) solutions whenever cost-effective and valuable to do so.
- Establish, operate, and maintain Records Management capabilities (processes, procedures, and tools) to create, receive, validate, maintain, catalog, store, update, and retrieve data IAW DoD and CCMD Policy and Procedures.

C.5.2.2.5.2. EUCOM KNOWLEDGE MANAGEMENT (KM)

The Government requires dedicated Knowledge Management practioners to support command decision-making. The Contractor shall apply KM expertise to meet EUCOM objectives, to improve collaborative information sharing, and to support the EUCOM's vision of superior mission execution through comprehensive shared understanding among USEUCOM and all partners. The vision of the EUCOM

Information Superiority and Knowledge Management (ISKM) division is to develop KM solutions using agile methodology embodying best UI/UX principles.

The Contractor shall, consistent with technical direction provided by the Government:

- Provide KM expertise to manage and guide the EUCOM KM program.
- Employ expertise in software and hardware engineering in partnership with business process engineers to develop and maintain appropriate solutions to identified demand signals.
- Perform process analysis and modeling employing related disciplines such as requirements analysis, outreach/engagement, quality communications, strategic/systems thinking, etc.
- Perform requirements analysis, planning, design, integration, implementation, testing, deployment, documentation, and sustainment.
- Address interface/graphical design, database architecture, and enterprise systems integration requirements.

C.5.2.2.5.2.1. INFORMATION DISCOVER AND SHARING

In the KM discipline of Information Discovery and Sharing, the Contractor shall:

- Conduct analysis of information usage to elicit requirements, recommend possible courses of actions/solutions, and develop proactive information delivery solutions and techniques.
- Identify and implement business intelligence, reporting and data analysis needs in order to turn vast stores of data into information and knowledge in support of the command's decision cycle.
- Maintain and refine all elements of the metadata ontology and integration (terms, term store, taxonomy, application, supporting technologies, management processes, etc.) for the portal to remain accurate and relevant.
- Incorporate means by which machine learning can complement (and in many regards, replace) human categorization of information to aid adoption and ultimately speed discoverability.
- Respond to emergent information discovery/sharing requirements, providing solutions that offer the necessary agility to address the fluid nature of EUCOM operations.
- Develop solutions to enhance the command's decision-making processes and increase the speed and accuracy of the decision-making.

C.5.2.2.5.2.2. COLLABORATION

In the KM discipline of Collaboration, the Contractor shall:

- Provide technical support and oversight for the command portal on all domains (e.g., NIPR, SIPR, MPE, etc.)
- Expand integration of collaborative tools/services and assist EUCOM with the development and implementation of policies and practices on internal and external usage of these tools.

C.5.2.2.5.2.3. INFORMATION FLOW

In the KM discipline of Information Flow, the Contractor shall:

- Assist in enhancing the command's information flow through maintenance of the Battle Rhythm.

C.5.2.2.5.2.4. EDUCATION AND TRAINING

In the KM discipline of Education and Training, the Contractor shall:

- Provide specialized training for EUCOM senior leaders on KM principles and practices.
- Develop and deliver newcomer and refresher training to reach all EUCOM personnel.
- Develop and deliver advance practitioner training.
- Develop and deliver collaborative tool training as needed to support tools in use.

C.5.2.2.5.2.5. PROCESS IMPROVEMENT

In the KM discipline of Process Improvement, the Contractor shall:

- Identify critical processes across the staff and work with responsible elements to improve them.
- Develop means by which information can be commonly understood and applied across the spectrum of functions and planning horizons.
- Respond to emergent process improvement requirements to improve unforeseen process shortfalls/problems.

C.5.2.2.5.2.6. SOLUTION ENGINEERING

The Contractor shall:

- Evaluate technologies/solutions with consideration of the people and process solutions.
- Apply existing technology, if possible, before exploring new technologies.
- Consider and provide support recommendations that span the entire product lifecycle.
- Develop solutions – people/process, software, hardware - in conjunction with Business Process Engineers or Knowledge Management Experts (KMEs).
- Recommend use of Government- and Commercial Off-The-Shelf (GOTS/COTS) solutions whenever cost-effective and valuable

C.5.2.2.5.2.7. INTERNAL AND EXTERNAL OUTREACH PROGRAM

The Contractor shall develop and implement an Outreach program which includes:

- Facilitate monthly meetings between EUCOM and Knowledge Management Working Groups (KMWG) throughout the European theater.
- Plan, develop agendas, and chair the bi-weekly KMWG meetings between KM and the various Headquarters' J-codes.
- Conduct strategic outreach, as directed, to support synchronization of KM initiatives with internal and external partners.
- Attend and participate in the Joint/DoD KM forums, typically joined twice monthly via VTC and often after core business hours.

C.5.2.2.5.2.8. ADDITIONAL REQUIREMENTS

- The Contractor shall assist the Government with creating or editing plans and polices which codify KM principles, practices, procedures, and standards in various documents, guides, and instructions.
- The Contractor shall provide for Portfolio Management techniques in order to select, prioritize, and control KMs projects and programs in order to stay in line with EUCOM strategic objectives and KMs capacity to deliver. The goal is to balance change initiatives and business-as-usual while optimizing return.
- The Contractor shall maintain and update a test environment in order to sustain technical development.
- The Contractor shall provide sustainment functions for all KM solutions in the product portfolio.
- Software development shall follow the requirements identified in paragraph C.5.2.2.6 in this PWS
- The Contractor shall collect and document requirements unable to be met by existing KM capabilities, perform as application testers, and provide outreach to their assigned community of interest.

While being performance-based, to support these KM requirements it has been established that EUCOM ISKM:

- Requires a level of effort equal to a full-time dedicated KME for each J-code (J1-J9) for a total of 9 KMEs. (*Note: Each KME should have functional knowledge of the J-code they support (i.e. Personnel, Logistics, Budget, Communications and Information, etc.) along with SharePoint skills to allow them to assist the supporting J-code with Content Management, building groups, and developing or modifying workflows.)*
- Requests a minimum of two software development teams using an agile approach to development. The teams should be capable of working independently or collaboratively to achieve desired outcomes. At least one team shall be capable of SharePoint application development and the other team(s) capable of custom application (non-SharePoint) development. (*Note: Current agile methodology in use is Scrum; however, the Government would accept any rapid agile technology.)*
- Requests Data Scientist(s), Business Process Engineer(s), and/or Business Intelligence Analyst(s) to support the KM requirements.
- Requires a lab manager to maintain and configure/reconfigure the development lab.

Note: The disciplines identified above may not be all inclusive of the EUCOM KM requirements.

C.5.2.2.6. APPLICATION MANAGEMENT

The contractor shall provide lifecycle operation and maintenance application management support for each CCMD consistent with the DESMF (reference DESMF Edition III Section 10.3 Application Management). Under this section, it is anticipated that application management efforts will include modernization in continuing operations and current services and support for software releases that are categorized as iterations on the basic release and would not constitute significant performance improvements that expand the current performance envelope or extensive testing, such as DT or OT&E performed by an independent test activitiy. As such the requirements are considered maintenance efforts. Product improvements are expected to fall within the current performance envelope (per the definition of this term in the FMR). Development testing (DT) or operational test and evaluation (OT&E) by an independent operational test and evaluation agency is not anticipated. Unless funded by RDT&E appropriation, the services required under the scope of this Application Management section exclude requirements that increase the current performance envelope and exclude requirements for conducting Developmental Testing (DT) and Operational Test and Evaluation (OT&E) by and independent operational test agency (per FMR Volume 2A, Chapter 1, item 7 "Product Improvement").

C.5.2.2.6.1. RELEASE AND DEPLOYMENT MANAGEMENT

The Contractor shall:

- Create, update, and maintain a detailed Release Management Plan for Government approval.
- Perform integration, checkout, and deployment (release) to portal O&M team
- Construct, document, build, and track a release package for each release.
- Inform Government and other stakeholders of status, results, and implementation of releases.

C.5.2.2.6.2. SERVICE AND VALIDATION TESTING

The Contractor shall:

- Develop, update, and maintain a Service Validation Testing and Implementation Plan for release packages with review by the Government, and update as directed.
- Demonstrate compatibility with existing hardware and software before release and deployment.
- Conduct, monitor, manage, and document service validation and testing of all new/changed IT services following parameters in service design packages.
- Submit release packages with service validation and test results to Government for review and release approval.

C.5.2.2.7. WEB, PORTAL, COLLABORATION SERVICES

The Contractor shall provide web and portal services to include server infrastructure, database infrastructure, application deployment, software configuration, and portal customization. In addition, the Contractor shall provide collaborative user space within internally and externally managed web and portal services.

C.5.2.2.7.1. WEB SERVICES

The Contractor shall provide Web design and administration services to the CCMDs. The services include planning, designing, testing, and implementing static and dynamic Web pages, Web sites, Web applications and associated content. The Contractor shall deliver production management, Web page design, markup languages, scripting, and relevant Web services support. Web services changes to the Communications and IT baseline shall be planned and implemented IAW established, formal configuration management and change control processes. The Contractor shall apply knowledge, skills, and strong user interface design experience, along with Web development experience to:

- Ensure web content is designed using commercial best practices; final designs are subject to Government approval.
- Produce documentation and style guides (e.g. site maps, wire frames, mock-ups)
- Design, develop, and maintain a consistent information architecture, user interface features, site animation, and special-effects elements to ensure predictable, successful user interactions.
- Create scripts/code that interacts with Web servers, the content for Web-based systems, and provides dynamic Web content through the Web/internet servers.
- Seek user community feedback and input for improving and enhancing Web sites.
- Develop and implement standards/guidelines subject to Government approval.
- Advise and coordinate with content developers on requirements, and applicable standards.
- Research and recommend Web-technologies with respect to the distribution of content, collaboration, and information sharing.
- Identify and resolve technical issues with Web-based systems and content.
- Apply appropriate security measures; provide for the appropriate use of copyrighted material; and produce reports and other documentation.

The Contractor shall provide Web Services to AFRICOM's and EUCOM's Web-based systems for each respective Public Affairs Office.

C.5.2.2.7.2. PORTAL SERVICES

The Contractor shall provide Communications and IT support, including but not limited to, management, operations, and maintenance, for hardware and software identified by the Government as necessary for portal capabilities. The Contractor shall:

- Install, configure, and troubleshoot the production system and associated applications in all environments (i.e. Staging, Testing, Development).
- Perform system administration, domain administration, network administration and Lab engineering & administration.
- Support OS/Virtualization and other unique services which include Active Directory Federation Services (ADFS), Integration, REL, and Identity Management.
- Maintain system administration and day-to-day operations on the development network.
- Install, integrate, test, and deploy applications IAW approved test plans.
- Partner with application development team to help solve business needs.
- Administer and support infrastructure technologies in the Collaboration and Content Management space to include, but not limited to: CRM, Business Intelligence (BI), OCS/LYNC Skype for Business, MOSS, SharePoint.
- Upgrade the various technologies, as required.
- Complete assigned day-to-day support ticket requests for the above technologies.

C.5.2.2.7.3. COLLABORATION SERVICES

The Contractor shall provide Systems Analysis, Systems Engineering, System Administration, Information Assurance, and end-user support services for the Collaborative Information Environment (CIE) which includes primarily web-based tools required for collaboration, planning, and operational support. The Contractor shall:

- Oversee the SharePoint application portfolio on SIPR and NIPR networks
- Integrate / configure .NET applications and SharePoint technologies with SQL Server database
- Maintain the various SQL databases supporting Skype, CRM/TMT, and IIS/Web Applications
- Monitor performance of SharePoint architecture and web-based applications after implementation
- Serve as the central point of contact for SharePoint activities and acts as a liaison for users, content owners, team site administrators, and the Application Development team
- Advise the Content Librarian or Content Manager, and the Content Coordinator(s) on proper document profiling and customization for Corporation Portal (SharePoint);
- Perform SharePoint administration to configure settings that affect the system service, such as load balancing for indexes; to setting priorities for applications;
- Perform stress testing and other operations on the web storage system, the dashboard site, SharePoint servers and web parts, to assure optimal system performance
- Maintain application documentation to describe software components development, logic, coding, testing, changes, and corrections
- Assist the Application Development Team in the full lifecycle development of portal applications/parts including functional requirements, analysis, and user interface design, database design, security control setup, testing and documentation
- Operate and maintain desktop tools to provide end users with the ability to fully utilize the collaboration functionality such as Skype.

C.5.2.2.8. COMMAND AND CONTROL (C2) SERVICES SUPPORT

The Contractor shall deliver, operate, and manage Command and Control (C2) infrastructure IAW applicable CCMD Policy and Program Management Office guidance. The Contractor shall provide C2 systems applications and services support in the areas of systems engineering; server configuration; software engineering; and display management. This support is limited to what is allowable by Global

Command and Control System - Joint (GCCS-J) Program Management Office (PMO) or other designated C2 PMO.

The Contractor shall provide the following C2 systems support:

- Procurement of hardware with minimum specifications as determined by the PMO and GOTS developer.
- Proposed device connectivity as determined by the PMO and GOTS developer.
- Proposed rack space design for servers with proper cooling systems.
- Installation of GOTS and Government-provided equipment and software that is not proprietary and does not require specialized installation
- System Administration; System Maintenance; Technical Refresh/Upgrade Support
- Provide O&M virtual device management system and audio visual capability provided through ThinkLogical architecture.

C.5.2.2.9. INTERNET PROTOCOL TELEVISION (IPTV) SERVICES

IPTV is a COTS solution that provides users with the ability to view news and informational television channels on Multi-Format Set Top Boxes (MFSTB's) and/or the standard workstation. IPTV is a closed system that only requires one-way input from satellite channel receivers and the satellite dishes are 'receive only', without the ability to transmit. Since the information originates from a 'free-to-air' source providing public information via existing infrastructure, the information the system is capable of providing only Public access television.

The Contractor shall:

- Manage, operate, and troubleshoot IPTV equipment and infrastructure to include antennas, cabling, video distribution equipment, and end points.
- Establish an industry standard preventive maintenance schedule for the rooftop satellite equipment. Identify and establish a capability to both perform scheduled maintenance and respond to emergency requirements.
- Maintain the transceivers to industry standards
- Configure and maintain the satellite receivers to optimize the output for the desired channel
- Configure and maintain firmware of the encoders
- Configure and maintain all firmware updates for the IPTV Equipment located throughout the campus
- Perform all administrative and security tasks for the Virtual Machine Control Structure (VMCS) server
- Install, maintain, and administer the VMCS and media system applications required applications to provide IPTV services
- Perform all actions required when a new channel is requested
- Maintain adequate but not excessive sparing to support:
    - The maintenance needs of the transceivers, receivers, and encoders
    - New requirements and the maintenance needs of the IPTV Equipment

C.5.2.2.10. JOINT OPERATIONS CENTER (JOC) SUPPORT

The JOC facilities require physical and virtual device management as well as audio visual systems management IAW DoD and CCMD Policy, Procedures, and current architectures. Examples of systems within each facility include Unclassified, Classified, and Coalition workstations (e.g. desktop, laptop, VDI clients, and/or tablets), printers, AV desktop devices (e.g. Tandbergs), VOIP devices, IPTV, smart boards, and other peripherals.

The AFRICOM JOC consists of key operational rooms, including the Senior Decision Cell, the Watch floor, three Operation Center Rooms, three Action Cells, Conference Rooms, Team Rooms, Theater Rooms, Telecommunication Rooms, and the Alternate JOC.

The EUCOM Mission Command Center (EMCC) consists of key operational rooms, including Joint Operations Center (JOC), Senior Decision Cell, and the Focal Point Operations Center (FPOC). The JOC also contains 5 PODs in the JOC that can operate at multiple classifications levels and 1 NON-Class POD for special internet access. Additionally, the EUCOM Headquarters Conference Room and the Joint Network Operational Center are tied into EMCC Systems.

Given the importance and duty hours of these facilities, dedicated, on-site support will be required, as written. Periodic travel to Djibouti will be required for Contractor personnel supporting AFRICOM.

When feasible, efficient, and cost-effective, the Government will allow:

- Remote support networked-AV support for the Pentagon and SHAPE.
- Programming support from the Stuttgart area.

Logistical Considerations:

- Access to these facilities requires a Top Secret/Sensitive Compartmented Information (TS/SCI) clearance.
- Contractor employees that support the Networked-AV and VTC equipment must have, or obtain within 6 months, the Cisco CCNA Video as their 8570M Computing Environment certification with at least one FTE with a minimum of 1 year experience in installing, operating, and/or maintaining

ThinkLogical systems. Other certifications are subject to Government approval. Crestron (EMCC) and AMX (AFRICOM JOC) programing experience is desirable.

C.5.2.2.10.1. AFRICOM JOC REQUIREMENTS

Normal duty hours for dedicated support requirements to the AFRICOM JOC are Monday through Friday 0600-2200 local time. When services are required outside of normal duty hours due to mission needs, the Government should provide at least 24-hour notice.

The Contractor shall:

- Deliver, manage, operate, and monitor all networked-AV systems in the AFRICOM JOC. Example systems include the AV routing matrix, integrated computer systems, network infrastructure, and controlled lighting.
- Deliver weekly status briefs to AFRICOM JOC leadership on the status of networked-AV systems.
- Conduct user training on proper operation of networked-AV systems for AFRICOM JOC personnel.
- Develop, update, and maintain SOPs and operational guides on networked-AV systems operation.
- Develop and implement system operations checks for the AFRICOM JOC systems IAW CCMD Procedures.
- Develop and implement systems stress tests and implement them in coordination with AFRICOM JOC exercises. Develop a post exercise report with system reliability and performance details to include fix actions implemented or recommendations to mitigate future problems.
- Provide initial troubleshooting for any IT system/device within the AFRICOM JOC regardless of network and/or service provider.

For AFRICOM VTC Control Device Programming Services, the Contractor Shall:

- Deliver capability to develop, maintain, and update VTC Control Devices to meet end user customer requirements. The primary customers are the AFRICOM JOC and CJTF-HOA JOC, and as time allows the Programmer will support the various VTC rooms throughout CCMDs, HOA, the Pentagon, and SHAPE. For example, equipment supported includes ThinkLogical and AMX Control devices.

For the AFRICOM JOC Project Management Support, the Contractor shall oversee and manage all IT Service events and work orders that impact the AFRICOM JOC mission, regardless of the type or service provider. Examples of these duties include:

- Reporting system outages to the appropriate service provider and following up with status inquiries until service is restored.
- Reporting and coordinating necessary actions with equipment vendors for warranty, service visits, and/or repair work.
- Tracking, coordinating, and (when designated) acting as the AFRICOM JOC POC for all facility and IT Project actions which directly impacting AFRICOM JOC operations.
- Provide weekly briefings to AFRICOM JOC leadership on the status of all projects and actions being tracked.

C.5.2.2.10.2. EUCOM MISSION COMMAND CENTER (EMCC) AND JOC REQUIREMENTS

Normal duty hours for dedicated support requirements to the EMCC are 0700 to 2100 local time with an EMCC technician on telephone standby at all other times. In addition, when notified prior to or during real world operations or exercises, required on-site support may be extended to 24/7 coverage.

These Audio-Visual operations and maintenance tasks, while being performance-based, shall have a level of effort equal to two (2) dedicated FTEs.

- Deliver, manage, operate, and monitor all networked-AV systems in the EMCC. Example systems include the AV routing matrix, integrated computer systems, network infrastructure, controlled lighting, and associated peripherals.
- Deliver weekly status briefs to EMCC leadership on the status of networked-AV systems.
- Conduct user training on proper operation of networked-AV systems for EMCC personnel.
- Develop, update, and maintain SOPs and operational guides on networked-AV systems operation.
- Develop and implement a system operations checks for EMCC systems IAW CCMD Procedures.
- Develop and implement systems stress tests and implement them in coordination with EMCC exercises. Develop a post exercise report with system reliability and performance details to include fix actions implemented or recommendations to mitigate future problems.
- Perform initial troubleshooting for any IT system/device within the EMCC regardless of network and/or service device.

For EMCC VTC Control Device Programming Services, while being performance-based, shall have a level of effort equal to one (1) FTE:

- Deliver capability to continually optimize EMCC software coding, which controls numerous routable/VTC enclaves within the EMCC.
- Develop, maintain, and update VTC and Control Devices to meet customer requirements.
- Primary Customer is the ECJ3, and as time allows the Programmer may be tasked by ECJ3 to support the various VTC rooms throughout CCMDs, HOA, the Pentagon, and SHAPE. Support and maintain programmable equipment such as ThinkLogical routing matrices and Crestron Control devices.
- Assist in performing initial troubleshooting for any IT System/device within the EMCC regardless of network and/or service device.

For EMCC Project Management Support, the Contractor shall oversee and manage all IT Service events and work orders that impact the EMCC mission, regardless of the type or service provider, and shall have a level of effort equal to one (1) FTE. Examples of these duties include:

- Reporting system outages to the appropriate service provider and following up with status inquiries until service is restored.
- Reporting and coordinating necessary actions with equipment vendors for all EMCC procurement, warranty, service visits, and/or repair work.
- Tracking, coordinating, and (when designated) acting as the EMCC POC for all facility and IT Project actions which directly impacting EMCC operations.
- Deliver weekly briefings and associated product deliverables to EMCC leadership on the status of all projects and actions being tracked.

For the European Plans and Operations Center (EPOC) Operations Manager Support, the contractor shall coordinate and supervise all systems-related work in the EPOC to include work at the designated EUCOM ECJ3 COOP location(s), and shall have a level of effort equal to one (1) FTE. These duties may include:

- Lead and coordinate all necessary actions with systems such as Audio Video (AV) routing matrix, computer systems architecture, cabling infrastructure, and lighting arrays
- Coordinate/verify/deconflict with Garrison entities and other service/utility providers that the following EPOC and EMCC-integrated subsystems are fully operational in a non-interference

capacity to ensure the EPOC is fully operational and ready to support the EUCOM mission: HVAC, security, life safety, fire, grounding/lightning protection, plumbing, and electrical

- Brief the ECoS (EPOC Chief of Staff) on operational and project status and EPOC operations recommendations in order to support mission requirements
- Serve as the EPOC's operations manager to monitor, track, support, and collaborate as necessary with EPOC leadership, occupants, and especially the ECOS to ensure all integrated systems efforts are managed and executed
- Track, monitor, and deconflict contracts and agreements impacting all integrated EPOC systems, including but not limited to, structures, power/electric, HVAC, plumbing, fire suppression and physical security/alarms, and when applicable, report to EMCC Systems Chief for deconfliction and resolution with Garrison
- Track, monitor, report, and deconflict infrastructure metrics associated with maintenance rooms, technical rooms (TR) and utilities/communications closets/telecommunication rooms.
- Provide detailed plans for systems stress tests in coordination with EMCC exercises to provide EMCC leadership with integrated system reliability and performance details
- Manage all integrated systems work performed by vendors and other EUCOM programs of record to ensure work is complete and on schedule. Any deviations or problems will be reported to the EMCC Systems Chief.
- Provide technology recommendations for the expansion and integration of existing and new C2 (Command and Control) systems to support the EMCC mission. All solutions will be vetted to ensure compatibility with existing integrated systems technology.
- Provide weekly updates briefs and associated product deliverables to J3/EMCC leadership on the EPOC/EMCC systems and projects status
- Work with EPOC leadership to coordinate integrated systems support for daily operations to include exercises and real-world operational missions.
- Share knowledge and operations experience with facility support-related personnel fostering a team environment while ensuring all facilities and logistics operations are understood, executed, and maintained.
- Manage EMCC contract staff: AV Engineers, Project Manager, and AV Programmer

C.5.2.2.11. NETWORKED AUDIO-VISUAL (AV), VOICE AND VIDEO OVER IP (VVOIP) AND VTC SERVICES

Networked-AV, VVoIP, and Video Teleconferencing (VTC) services include hardware, software, network, and scheduling components necessary to deliver real-time voice and video communications between end-users at two or more locations. They include cameras, desktop cameras and enabling SW, coder-decoders (CODECs), monitors, onscreen menus, matrix switchers, control panels, speakers, microphones, near and far end camera control, screen-sharing, operation of the infrastructures, multi-point conferencing, and local and remote diagnostics. This covers both desktop and conference room networked-AV and VTC services.

The Contractor shall:

- Deliver, operate, and manage all aspects of conference room networked-AV, VVoIP, and VTC service operations including design, installation, configuration, programming, troubleshooting, and user interface IAW current architectures.
- Deliver, operate, and manage all aspects of desktop networked-AV, VVoIP, and VTC service operations including design, installation, configuration, programming, troubleshooting, and user interface IAW current architectures.

- Program switching fabric to enable control panel functionality IAW current architectures.
- Manage an enterprise VVoIP and VTC dial-plan (e.g. published on the CCMD Portal).
- Provide AV programming and engineering resources IAW customer requirements.
- Perform scheduling and manage Command assets used for scheduling and bridging events with internal and external users.
- Perform set up and operations, multi-session bridging, and other related administrative tasks to enable connectivity both with internal and external participants.
- Configure and manage display systems for interoperability with external networks.
- Provide end user support in operating equipment and in establishing, maintaining and troubleshooting connectivity throughout the duration of the video-conferencing session. Support both point-to-point and simultaneous point-to-multi-point connections.

C.5.2.2.12. IP VOICE SERVICES

Voice Services enables voice communications over an IP network interfaced with the Public Switched Telephone Network (PSTN). The Contractor shall:

- Perform local touch-labor installing, removing, or replacing Voice over Internet Protocol (VoIP) and Voice over Secure Internet Protocol (VoSIP) end user devices
- Troubleshoot end user devices to determine malfunction, reconcile whenever possible or pass incident to the service provider
- Perform account management functions as designated by the service provider

C.5.2.2.13. MOBILITY COMMUNICATIONS SERVICES (PHONE AND TABLET)

The Contractor shall:

- Procure, inventory, track, provision, issue, lifecycle, and troubleshoot classified and unclassified mobile communications devices. For example, Defense Mobility Unclassified Capability (DMUC) end user devices, DISA Defense Mobility Classified Capability (DMCC) end user devices, laptops, tablets, hot spots, and voice-only devices. This may require coordination with external entities.
- Configure mobile devices IAW DoD and CCMD Policies and Procedures.
- Ensure secure access to unclassified and classified services. For example, secure email services.
- Manage delivery of commercially contracted mobile services IAW DoD and CCMD Policies and Procedures.
- Analyze mobile service bills to identify and recommend areas for cost-savings or capability increases.
- Verify that only authorized users have been issued mobile devices and that authorized users maintain positive physical control IAW DoD and CCMD Policies and Procedures.

C.5.2.2.14. INFRASTRUCTURE AND APPLICATION SYSTEMS ADMINISTRATION SERVICES

The Contractor shall provide continuous system administration services for CCMD designated information systems as shown in the attachments for each CCMD. All Contractor-provided IT services will be implemented and operated IAW all applicable DoD Policies and Instructions. These services consist of Infrastructure System Administration, Application System Administration, System Security, and System Capacity Planning tasks.

C.5.2.2.14.1. INFRASTRUCTURE (OS) SYSTEM ADMINISTRATION TASKS

The Contractor shall:

- Configure devices and OS IAW applicable security policies and procedures

- Apply OS updates, patches, and configuration changes or in the case of automated updating (i.e. SCCM) ensure schedule actions were completed
- Analyze system logs to identify potential issues with devices or systems
- Perform routine audits of systems, OS, and software.

C.5.2.2.14.2. COMMON APPLICATION SYSTEM ADMINISTRATION TASKS

The Contractor shall:

- Install and configure application IAW applicable security policies and procedures.
- Analyze system logs to identify potential issues with the application or system.
- Perform routine audits of application software.
- Perform backups (see System Storage Capacity Planning).
- Manage (add, remove, or update) user account information.
- Respond to technical queries and assist users, as required.
- Document the configuration of the system.
- Troubleshoot any identified or reported problems.
- Perform system performance tuning, when authorized.
- Configure, add, or delete File Systems.

C.5.2.2.14.3. SYSTEM SECURITY TASKS

The Contractor shall perform the following system security tasks:

- Take appropriate measures to respond to known and possible network attacks IAW applicable DoD policies, directives and instructions, or as directed by the Cyber Service Provider (CSSP).
- Ensure all Contractor managed items are configured to store and archive all system, device, application, and security event logs IAW DoD and (if applicable) NATO security policies.
- Audit and review all system, device, application, and security event logs IAW DoD and (if applicable) NATO security policy.
- Report, mitigate and/or resolve all classified security incidents (e.g. data spills) that impact CCMD networks within time constraints identified by the applicable directive or as directed by the CSSP.
- Supporting incident reporting activities IAW CSSP and CCMD policies
- Support and provide the necessary information (i.e. firewall logs, system logs, storage media, etc.) to the Government designated organizations in the performance of forensic analysis services.

C.5.2.2.14.4. SYSTEM STORAGE CAPACITY PLANNING

The Contractor shall provide the following storage capacity related services:

- Identify system and application needs to obtain required storage then configure the system/application to store data in the allocated space.
- Manage allocated storage to avoid incidents caused by lack of capacity; justify and request additional storage should it become necessary
- Follow the Disaster Recovery plan to ensure there is no application performance degradation should a DR event occur

C.5.2.2.14.5. SPECIALIZED APPLICATION SERVICES

Some applications require more support which is provided by this PWS section. It is anticipated that a SME in the capabilities and usage of these products may be required to assist the client(s) with these applications. These applications are listed below:

C.5.2.2.14.5.1. TASK MANAGEMENT TOOL (TMT)

The Government specialized application services for the Task Management Tools (TMT) is implemented by stakeholder organizations supported under this Task Order. The scope of this support includes providing technical assistance with the installation, integration, configuration, and administration of the respective tools; maintaining the server and operating system; managing the database; providing database administration support to maintain the structure and integrity of the tool/data; providing for the operations and maintenance of the tools to ensure the operational availability and integrity of the data; and provide end user training and assistance. The Contractor shall:

- Provide CRM/TMT Solution Management by validating that solutions are tested prior to deployment. Develop and implement mitigation plan for all solutions. Regularly monitor system utilization to ensure the most cost effective license management.
- The contractor shall develop management scripts for automating routine administration tasks within CRM and inform government representative of CRM/TMT critical migration paths and associated risks. The contractor shall complete upgrades as directed by the government.
- Provide problem escalation consisting of contacting the Accenture TMT Service Desk as provided in the Accenture's Software Maintenance Agreement. Once reported, the Contractor shall keep the Government informed of progress until resolution. *(Note: Prior to incurring any additional cost from Accenture, the Contractor must obtain Government approval.)*
- Provide user training to the mission owner as required and as a minimum one-hour block of instruction twice a month during Action Officer Training. The contractor shall ensure the training covers task creation, delegation, routing, response and closure.
- Assist users in determining business processes, establish hierarchical process mappings for taskings and awards workflow, develop workflow and routing within parent organizations, and continually review TMT configuration to ensure efficient and logical results. The contractor shall assess and develop command routing topologies to ensure the fullest investment in the CRM infrastructure and provide solutions to new and unique business requirements.
- Plan and coordinate the Accenture TMT Engineering site visits to perform system maintenance and when required system upgrades. The Contractor shall ensure all stakeholders are kept informed to minimize impact during these visits/upgrades.

C.5.2.2.14.5.2. HP TRIM

The Contractor shall serve as the technical expert for all matters pertaining to records management and the secure operation of the TRIM electronic records management application. The work requires sound knowledge of research methods and data analysis techniques. The scope of this work includes:

- Creating and managing end user accounts, inclusive of: registering and troubleshooting user profiles to ensure login capability, impose access controls, verify credentials, and maintain controlled access to documents and content within the ERM application.
- Training AFRICOM end users on the TRIM application and records management.
- Assist with the collection and preservation of official classified and unclassified records, electronic versions, relating to day-to-day and operational documents in a manner that meets governance and regulatory compliance requirements for records retention.
- Supporting problem identification and resolution.
- Responding to and providing timely resolution of trouble tickets providing Tier III technical support to resolve incidents
- Providing consultative support, as requested, to develop and/or recommend standards for the Command's Electronic Records Management system.

- Participating in Staff Assistance Visits (SAVs) and assisting with drafting SAV reports. The SAVs provide a comprehensive measurement of organizational compliance with all applicable records management regulations, and provide formal documentation as to compliance, discrepancies, and suggestions for improvement.
- Assisting with facilitating the review and collection of records accessed that have permanent historical value under title 44 United States Code, (U.S.C.) pursuant to the provision for automatic declassification in Section 3.3 of E.O. 12958.

C.5.2.2.14.5.3. CYBERARK

DoD has mandated the use of PKI authentication for all accounts on DoD networks; however, until recently this has not been possible, as there are several technologies in use which are not PKI enabled. With DISA's addition of CyberArk to the Approved Product Listing, CyberArk is the DoD tool to authenticate using PKI on technologies that support PKI natively is now possible. Both CCMD's have chosen to implement the CyberArk solution to be compliant with the DoD PKI mandate, better the security posture of the networks, and increase their Cyber Scorecard ratings.

CyberArk is a PKI enabled service which acts as an authentication proxy to broker connections to non-compliant technologies (e.g. devices, servers, appliances, and/or applications). It securely manages passwords for both privileged and non-privileged service accounts, and serves as the operations password vault for emergency accounts.

The Contractor shall provide engineering, integration, and operations & maintenance for NIPRNet and SIPRNet, to include, but not limited to:

- CyberArk server components and hardware security modules
- Onboarding and the maintenance of privileged administrator accounts within CyberArk
- Managing service accounts through CyberArk to meet DoD requirements
- Configuring and maintaining native connectors to non-PKI devices
- Preforming System Administration and System Security
- Integrate new technologies into the CyberArk solution set as well as validating existing solutions continue to work when supported technologies are upgraded
- Integrate custom connectors when necessary for non-PKI technologies
- When new/additional CyberArk capabilities/features are available, the Contractor shall implement these capabilities
- Provide for a tiered approach to troubleshoot and repair the offering should problems occur to include working with technology owners for problem resolution

Note: The term "connector" refers specifically to Privileged Session Management (PSM) Connectors which leverages macro-like scripting techniques. Not currently covered is the Central Policy Management (CPM) Plug-Ins. Should CPM Plug-ins be required in the future, the Government will provide more detailed requirements for support.

C.5.2.2.14.5.4 SERVICENOW

As a maturation of the CCMD's IT Service Delivery, the CCMDs have implemented the IT Service Management and Process Automation System, ServiceNow, as an integrated solution to automate, add efficiency, gain better visibility, and monitor and control the CCMD's IT services and portfolios. The Government has an operational need to maintain, integrate, and expand the use of the ServiceNow system in order to facilitate the delivery of IT services in the organization.

The contractor shall provide system administration for maintaining the stability and usability of the ServiceNow platform by performing application maintenance, managing support for incidents related to ServiceNow applications, and contributing to ServiceNow software releases by delivering configuration tasks and features. The contractor shall enable the fulfilment of common configuration and maintenance tasks associated with the ServiceNow platform.

The contractor shall:

- Responsible for core system configuration and administration of ServiceNow:
- Develop and maintain workflow customizations.
- Facilitate rollout of new applications and modules.
- Handle general updates and configuration changes/requests.
- Identify system deficiencies and recommend solutions.
- Provide maintenance and continuous improvement of the processes, standards, policies, working methods, and tools.
- Build and execute automated test procedures and scripts, and participate in associated testing (both verification and validation) activities.
- Develop and maintain integrations between ServiceNow and other information systems with an understanding of REST, SOAP, web service architectures.
- Assist in the implementation and enhancement/customization of ServiceNow modules and features (e.g., CMDB, Knowledge, Discovery, Orchestration) based on process owners' needs.
- Assist with the build and support of business solutions that align with the enterprise IT Service management strategy.
- Design, publish, and maintain service catalog items in accordance with customer requirements.
- Create, maintain, and manage customer experiences via portals, pages, and items.
- Manage core foundation data, tables & columns, and configuration item (CI) classes.
- Accurately create, test, and manage update sets in a high paced environment.

~~[AFRICOM only]~~ The contractor shall provide subject matter expertise in ServiceNow system applications and custom applications. The contractor shall work with Government process owners and partner integrators to maintain system operations, resolve issues and incidents, and enhance or improve the system. The Contractor shall provide engineering, integration, and operations & maintenance for NIPRNet and SIPRNet ServiceNow, to include:

- Work with both Government leadership and external providers to research, analyze, and implement enterprise-wide network security solutions/capabilities/enhancements to support CCMD mission, goals and objectives.
- Create custom dashboards in ServiceNow integrating and combining data from multiple tables and sources based on user requirements.
- Create custom reports and searches in ServiceNow based on user requirements.
- ServiceNow security fundamentals and approaches including integration with other systems.

- Create, maintain and enhance Incident Management, Problem Management, Service Request Management, Service Catalog, Knowledge Management, Self-Service Portals, single sign on (SSO) capability, and Active Directory Profile synchronization.
- Create, maintain and enhance team Dashboards and reporting, including scheduled reports.
- Oversee, maintain and enhance Change Management, as well as current connections between ServiceNow and other systems.
- Maintain Forms, Reports, Views, Workflows, Groups and Roles.
- Coordinate application and platform upgrades.
- Document and/or analyze business processes and translating to system and technical requirements for implementation.
- Execute adaptive, corrective, and preventative changes to the platform, platform applications, and interfaces to the platform to include creating, modifying, documenting and maintaining ServiceNow core components.

C.5.2.2.14.5.5. F5 SUPPORT SERVICES [AFRICOM ONLY]

F5 hardware and software products have been incorporated within the AFRICOM network and have mission-essential features for the enterprise application delivery deployment; supporting DMZ to provide a secure gateway through route domains, F5 firewall (WAF), F5 Application firewall (ASM), Sec-DNS for global load balancing through F5's GTM (global traffic manager) and access control lists. The Contractor shall serve as the technical expert for all matters pertaining to the operation, configuration, and maintenance of F5 systems in a multi-enclave environment. In supporting the F5 infrastructure, the Contractor shall:

- Architect, analyze, plan, and design the configuration and expansion of the F5 infrastructure.
- Leverage network and F5 expertise to provide on-going network support, tune performance, and address availability issues of appliances and infrastructure.
- Guide operations and engineering staff for AFRICOM solutions involving the F5 infrastructure.
- Develop courses of action (COAs) for the life cycle refresh of current F5 appliances.
- Perform high-level troubleshooting tasks involving the F5 infrastructure including connectivity issues and replacing failed hardware.
- Rapid identification, troubleshooting, and resolution of hardware and software issues and events in order to minimize customer impacts, which requires providing monitoring of the F5 infrastructure and related services to predict and preemptively prevent issues and events that adversely impact delivery of services to customers.

Respond to break-fix incident requests for F5 related issues and coordinate with system and network administrators to eliminate F5 appliances as a potential cause in break-fix incident requests.

C.5.2.2.15. NETWORK SERVICES

The Contractor shall maintain and provide network connectivity by networks and systems to ensure mission critical systems and operations are available with the goal of achieving Government established monthly availability rates, not including authorized or planned service interruptions or preventive maintenance. The Contractor shall monitor and report network operational status and posture 24/7/365 in accordance with CCMD directives. The Contractor shall provide Network Management Services to include those hardware and software standards, solutions, processes, and services which encompass:

C.5.2.2.15.1. WIDE AREA NETWORK (WAN) SERVICES

The Contractor shall Operate, maintain, and manage the WAN infrastructure between DISA-provided circuits and the LAN infrastructure. The Contractor shall:

- Configure devices in accordance with security policies; maintain and update OS and firmware, as required.
- Monitor and report operational status; resolve connectivity issues when they occur to include assisting the service provider (i.e. DISA) with troubleshooting.
- Develop and maintain IP address schemes for all assigned networks under their addressing control.
- Annually review and update (as needed) the Master IP Routing Schema.
- Manage circuit provisioning throughout the delivery lifecycle from origination to discontinuance.
- Install and test circuit and base extensions; coordinate with external entities (e.g. DISA) and the Government manager for end-to-end testing and activation.
- Provide capacity and utilization monitoring (e.g. WAN access circuit capacity, WAN subscription capacity).
- Conduct annual service continuity site assessments, identify deficiencies to include single points of failure, and recommend architectural and design modifications.
- Install, configure, key, re-key, and manage NSA Type 1 Encryptors.

C.5.2.2.15.2. LOCAL AREA NETWORK (LAN) SERVICES

The Contractor shall operate and maintain the LAN infrastructure including all supporting equipment (e.g. switching and routing devices, firewalls, load balancers, alarmed carrier devices, uninterruptible power supplies, in-line network encryption devices, etc.). The Contractor shall:Configure network devices in accordance to applicable security policies and procedures; update OS and firmware, as required.

- Operate and maintain the network devices to achieve a normal, continuously operational state.
- Plan, schedule, and implement maintenance actions to sustain the operational viability of the networks, to include forecasting technology refreshment/insertion projects.
- Install, configure, operate, and maintain firewalls, load balancers, network management systems, and network sensors, as required.
- Install, configure, key, re-key, and manage NSA Type 1 Encryptors.
- Create, maintain, and manage VLANs as necessary to support Access Control List requirements.
- Operate and maintain Multi-Protocol Label Switching and Quality of Service (QOS) where enabled.
- Comply with the DoD Ports, Protocols, and Services directives for configuration of assigned transport infrastructure.
- Troubleshoot and correct all detected or reported network faults.
- Provide Trending and Capacity Planning services to analyze and plan for the efficient utilization and management of the networks.
- Notify the Government if the addition of a network device or service will exceed 75% of existing port capacity, transport infrastructure element (e.g., rack space), inside cable plant, or outside cable plant utilization.
- Conduct annual service continuity site assessments, identify deficiencies to include single points of failure, and recommend architectural and design modifications.

C.5.2.2.15.3. REMOTE ACCESS SERVICES (RAS)

The Contractor shall operate and maintain RAS infrastructure to provide secure access to enterprise services from remote locations. The Contractor shall:

- Operate and maintain Dynamic Multimode Virtual Private Network (VPN) to enable enterprise access for designated remote sites.
- Operate and maintain Remote Access VPN to enable individual end users remote access to enterprise services.

C.5.2.2.15.4. JOINT REGIONAL SECURITY STACK (JRSS)

The Contractor shall:

- Manage and operate JRSS suites IAW DoD and CCMD Policies and current architectures.
- Manage JB-CE router pairs using Joint Management System (JMS) tool suite and DISA mandated applications.
- Coordinate with external entities (for example, DISA, RCC-E) in support of JRSS operations and migrations.

C.5.2.2.16. VIRTUAL DESKTOP INFRASTRUCTURE (VDI) SERVICES

The Contractor shall be responsible for O&M on all servers, storage, applications, and network equipment as identified. O&M services encompass support for the current Phase 1 VDI server environment, VDI Storage Area Network, CITRIX desktop environment as well as user end points connected to the network.

The Contractor shall:

- Provide, manage, and operate end-to-end VDI IAW current architectures.
- Provide Operations and Maintenance support to include applicable IA services for the CCMD's VDI infrastructure for desktop presentation in single or multi-level security environments.
- Test and integrate virtualized operating systems, middleware, and applications.

C.5.2.2.17. VIRTUALIZATION

The Contractor shall:

- Meet or exceed CCMD goals for data center virtualization.
- Provide, manage, and operate virtualization services, to include virtualization infrastructure (VI), hardware, and middleware IAW current architectures.
- Test and integrate virtualized operating systems, middleware, and applications.

C.5.2.2.18. STORAGE SERVICES

The Contractor shall:

- Manage and operate the storage infrastructure including hardware, software, processes, and tools.
- Provide end users with the ability to store and retrieve files on shared and controlled-access storage media.
- Perform data replication and data deduplication IAW CCMD Enterprise Storage Procedures and NIST Standards.

C.5.2.2.19. CROSS DOMAIN SOLUTION (CDS) SERVICES

Cross Domain Solution (CDS) Services provide either access to or transfer of data between different security domains enabling the exchange of information across national, security, and management domain boundaries. The Contractor shall implement and manage CDS, including user account management IAW DoD and CCMD Policies and Procedures

C.5.2.2.20. COMMERCIAL SOLUTIONS FOR CLASSIFIED (CSfC)

The Contractor shall:

- Deliver, operate, and manage technical solution to provide remote access to classified networks and services over approved CSfC devices IAW CCMD Policies and Procedures.
- Develop compliance reports for CSfC equipment IAW DoD and CCMD Policies and Procedures.
- Schedule and conduct training of CSfC technical solution.

C.5.2.2.20.1. EUCOM FLAGSHIP NETWORK

The Contractor shall be responsible for the FLAGSHIP network, SIPR services accessed by the end user, and the end user device to include the baseline software. The end user CSfC connection provisioning to include documentation and training, along with end user support for connecting the devices is the responsibility of the designated Government entity. The Contractor shall provide engineering and O&M service for FLAGSHIP to include:

- The Government may request integration CSfC into the Executive Communication Kits.
- Network and System Administration of FLAGSHIP to include performing certificate authority duties for both the red and grey networks.
- Service desk response for all Flagship calls to include triaging incidents and problem elevation.
- Perform as the Flagship Security Auditor, which in addition to Cybersecurity tasks, specific tasks include:
  - Conducting NSA Required Weekly Compliance Auditing.
  - Use the Dell Data Protection Encryption to manage DAR solution.
  - Audit and maintain End User Device agreements.
  - Perform all CSS functions for the CSfC network to include incident handling, response, and reporting. *(Note: Report all incidents to the designated NSA POC and IAW EUCOM procedures.)*

Note: One individual cannot perform Certificate Authority duties for both networks on a single request. The Security Auditor is only authorized access to audit logs and may not perform system administration duties on the CSfC grey network or as a Certificate Authority on either network.

C.5.2.2.21. CRYPTOLOGIC SUPPORT/SECURITY

The Contractor shall:

- Provide cryptographic equipment and lifecycle support to include design, transition, securing and operating government procured COMSEC equipment.
- Manage, safeguard, and maintain accountability for Government-provided cryptographic/encryption products and keying materials and perform cryptographic equipment support services IAW the authoritative COMSEC Management user account guidelines and training.
- Manage National Security Agency Type 1 encryption devices and other National Security Agency approved encryption devices when requested.

C.5.2.2.21.1. EUCOM CEKMS (COMSEC)

The contractor shall provide O&M service to Coalition Electronic Key Management System/Key Management Infrastructure (CEKMS/KMI), which includes:

- Conducting receipt, transfer, destruction, and inventory of electronically received COMSEC keys. EUCOM provides support via NSA help desk support and annual vendor support.
- Serve as an advisor (CEKMS/KMI SME) regarding all COMSEC issues and liaison between the CCIB COMSEC Accounts based on guidance or direction of the Government.
- Manage COMSEC IAW the authoritative COMSEC Policy and Procedures. Management tasks consist of operating and maintaining current and future COMSEC equipment such as, a Coalition Electronic Key Management System (CEKMS), the Key Management Infrastructure (KMI) system, and Tier 3 Key Loader devices. Contractor personnel shall receive technical direction (coordination and instructions) from the Government on all issues concerning COMSEC equipment, keys and associated programs released to partner nations.
- Perform COMSEC Manager and Alternate COMSEC Manager duties IAW NSA CSS Policy Manual 3-16.
- Perform COMSEC audits and inspections when required and at the direction of Government.
- Develop Emergency & Precautionary Destruction Plans and Emergency Action Plan (EAP) and Standard Operating Procedures (SOP) for Government approval.
- Contractor shall conduct exercises of the COMSEC account EAP(s) per NSA CSS Policy Manual 3-16.

C.5.2.2.22. CYBER SECURITY

All Contractor-provided IT services will be implemented and operated IAW all applicable DoD Policies and Instructions, Security Technical Implementation Guides (STIGs), Security Requirements Guides (SRG), Best Business Practices, vendor security guidance, Information Conditions (INFOCON), DoD Task Orders, and CCMD Policies as they are updated or newly implemented.

C.5.2.2.22.1. CYBER SECURITY OPERATIONS

The Contractor shall:

- Operate tools and systems that are required to support the CCMD cybersecurity program and its functions IAW current architectures. This includes all hardware and software tools and sensors from perimeter to endpoint, as applicable. For example, network intrusion detection systems, endpoint security software, Host Based Security System / ePO servers, and web proxy.
- Evaluate and implement all applicable DoD orders and directives to include, but not limited to the Information Assurance Vulnerability Management (IAVM) Program, TASKORDs, GENADMINs, OPORDS, EXORDS, INFOCON changes, Coordinated Alert Messages (CAMs), CCMD-approved Risk Mitigation Plans (RMP), as directed.
- If compliance cannot be met on any order or directive, provide a Plan of Action and Milestones (POA&M) to the Government for approval within the directed timelines.
- Test and evaluate software security patches and security-related configuration changes for compatibility with the current baseline and resolve any conflicts prior to deployment.
- Monitor implemented security controls and report status, IAW the approved CCMD Continuous Monitoring plan.
- Perform and document Risk Assessments of findings (for example, vulnerabilities, non-compliant areas) identified through Continuous Monitoring Activities. Recommend courses of action for addressing all findings.
- Develop CCMD cyber security policies for Government approval.
- Review existing cyber security polices and develop recommendations, as required.
- Evaluate, from a security perspective, new, replacement, trial, or test equipment or software being brought into authorization boundaries.
- Manage CCMD Exceptions to Policy workflows for Portable Electronics Devices. All Exceptions to Policy require Government approval.
- [AFRICOM only] Provide expert guidance, direction and execution of information security management activities to include:
    - Apply continuous monitoring techniques to evaluate system security posture.
    - Ensure appropriate operational security posture is maintained.
    - Develop and maintain System Security Plans (SSPs), policies, procedures, and best practices.
    - Work with Designated Authorizing Official (DAO) to ensure systems obtain and maintain accreditation.
    - Ensure emergent systems are compliant during engineering and integration, prior to transition into operations and maintenance.
    - Perform audit reviews and compliance reporting.
    - Conduct reviews of information systems to ensure security compliance.
    - Implement and support all phases of Risk Management Framework (RMF).

C.5.2.2.22.2. COMPLIANCE REPORTING

The Contractor shall:

- Track and report status on all applicable orders, directives, and Plans of Actions and Milestones (POA&M).
- Ensure required compliance reporting is published in the authoritative systems of record IAW DoD and CCMD Policies.
- Perform periodic and on-demand required scans (eg. vulnerability, unauthorized software) on all CCMD assets, including POR systems, following the Government-approved procedures and using the Government approved tools (currently using Assured Compliance Assessment Solution (ACAS).
- Provide scan results to service providers external to this task order for systems under their purview.
- Obtain vulnerability scan configurations and results from external service providers or end-user prior to authorizing a guest end user device access to EUCOM.
- Maintain scanning results and develop vulnerability trend reports IAW DoD and CCMD procedures.
- Perform and maintain system registrations IAW DoD and CCMD Policy. These registrations include, but are not limited to, those in the Ports, Protocols, and Services Management (PPSM) database, Systems/Network Approval Process (SNAP), DoD NIPR DMZ Whitelist, and DoD IT Portfolio Repository (DITPR).
- Compile information and support required for cyber evaluations, inspections, assessments, and reporting tasks, as directed, such as the Joint Staff Cybersecurity Scorecard.
- Track the implementation status of recommended/required actions derived from exercises and inspections, as directed.

C.5.2.2.22.3. CYBER SECURITY INCIDENT RESPONSE

The Contractor shall:

- Report potential cyber security incidents or anomalous system events IAW DoD and CCMD Procedures.
- Perform incident response actions, as directed IAW CCMD Cyber Security Incident Response Plan. These actions may include, but are not limited to system isolation, data gathering, reimaging machines, physically removing hard disk drives, and evidence handling IAW CCMD Procedures.
    - Report status of incident response actions IAW CCMD Cyber Security Incident Response Plan.
    - Develop recommendations for countermeasures or process improvement based on lessons learned in support of incident response.
    - Develop plans or response strategies to cyber security incidents and implement the appropriate activities to limit incident impact and restore any capabilities or services that were impaired due to a cyber security incident.
- Perform response actions to instances of other security incidents, for example, Unauthorized Disclosures of Classified Information (UDCI), Cross-Domain Violations, and Unauthorized Activity, as directed, IAW DoD and CCMD Procedures.

C.5.2.2.22.4. ENTERPRISE LOGGING

The Contractor shall:

- Implement enterprise logging IAW STIGs, DoD and CCMD Policy, and current architecture to include:
  - Configure and tune endpoint log generation.
  - Configure and operate centralized logging solution.
  - Configure and maintain connections for the forwarding of logs to Cyber Security Service Provider (CSSP).
  - Validate that logs are retained and available and report results.
- Audit logs and report audit results to the Government IAW DoD and CCMD Procedures.

C.5.2.2.22.5. RISK MANAGEMENT FRAMEWORK (RMF)

The Contractor shall:

- Manage the RMF program for the information systems under the purview of the CCMD.
- Perform technical writing to develop, update, organize, maintain, and track required RMF documentation. Examples include technical documents, templates, support agreements, exceptions to policy, diagrams, and illustrations.
- Coordinate with internal and external stakeholders to obtain and organize required documentation.
- Manage and maintain the RMF Assessment and Authorization (A&A) program
- When there is a significant change to the system's security posture, the Contractor shall update the current authorization package, or obtain a new authorization, if required.
- Obtain, maintain, and manage A&A documentation for External Systems (for example, Program-Managed Systems) for connection authorization via cybersecurity reciprocity.
- Obtain, maintain, and manage A&A documentation for Cross-Domain Solutions for connection authorization.
- Develop A&A documentation for Government approval, as directed, IAW DoD and CCMD Policies.
- Populate, maintain, and provide access to all cybersecurity A&A documentation in the authoritative location (for example, Enterprise Mission Assurance Support System (eMASS) and Xacta IA Manager).

C.5.2.2.22.6. SECURITY CONTROL ASSESSMENTS (SCA)

The Contractor shall:

- Perform Security Control Assessments of software and hardware being considered for the command's Approved Product List. Make recommendations on alternatives or configuration changes that help meet the required capability in a secure manner.
- Perform on-site Security Control Assessments on CCMD networks and systems, as directed, and report findings to the Government.
- If compliance cannot be met on any Security Control, develop and submit a POA&M or Exception to Policy, as directed, to the Government for approval within the directed timelines.
- Perform and document Risk Assessments of findings (vulnerabilities, non-compliant areas, etc.) identified through Security Control Assessments. Recommend courses of action for addressing all findings.

C.5.2.2.23. ENTERPRISE ARCHITECTURE SUPPORT

The Contractor shall:

- Develop, integrate, and keep current CCMD architectures and views (for example, OV-1, SV-1) to include graphically documenting all architectures/topologies IAW CCMD-directed framework and formats.
- Develop reference and objective architecture(s) for CCMD networks.
- Maintain architecture products and network diagrams in designated command repositories.
- Conduct and document assessments of Service Component architectures and make recommendations to improve IT service interactions, as directed.
- Use CCMD-approved enterprise architecture tool(s).

C.5.2.2.24. SYSTEMS ENGINEERING SUPPORT

The Contractor shall provide Network and System Engineering Support services to enhance customer service, to maintain/improve system performance, and to ensure reliability for the C4 Networks and Systems for projects as designated by the CCMD.

The Contractor shall provide services to resolve performance and reliability challenges that emerge as the C4 Network and System continues to evolve and undergo modernization. Engineering also ensures a structured problem-solving approach. The Contractor shall:

- Perform all required engineering functions found in the Service Design Domain and provide escalated support to incident management.
- Deliver services required for sustaining the transmission and/or communication path between geographically separated users/devices. For example, satellite, leased lines, and wireless.
- Install, configure, and transition IT systems to IT Operations Management.
- Integrate and ensure interoperability of end user computing devices (e.g. desktops, laptops, and other portable devices) and peripherals with supported networks and communities of interest.
- Ensure IT system interoperability across the CCMD enterprise and with external systems.
- Develop dashboards displaying the status of the enterprise using outputs from existing IT tools (e.g. SCCM, SCSM, What's Up Gold, Spunk, Cisco ISE/Prime), when directed.

The Contractor's engineering processes will span other areas of this PWS. Logistical support areas such as tool purchasing, asset management, and configuration management will be integral to many of the engineering projects. The Cyber Security service area of Security Control Assessments will assure that required security controls are addressed in the solution.

The Contractor may or may not have full control of the Engineering projects they are assigned. Depending upon the scope, size, complexity, and Government needs, the Contractor will often be a member of an integrated team consisting of both Government and other Contractors. Project plans will clearly identify the Contractor's roles and responsibilities.

The Government anticipates the need of the following disciplines in performance of engineering tasks:

Application Integration
Audio Visual Engineering
Data Architecture Engineering
Data Base Design and Architecture

Network Engineering
Project Management
Server Infrastructure Engineering
Storage Infrastructure Engineering
System Engineering
Technical writing
Unified Communication Engineering

Note: The disciplines anticipated may not be all inclusive. Additionally, inclusion of a discipline does not indicate that one FTE (a full man-year) is needed in that area nor on the other hand that one FTE will suffice.

C.5.2.2.24.1. CAPABILITIES PLANNING AND REQUIREMENTS ANALYSIS

The Contractor shall assist the Government by providing forward-thinking technical direction and engineering services for assessing system performance and business needs, planning for new and evolving C4 systems, evaluating proposals for the migration of existing services, and making recommendations for corrections and enhancements to current systems. Contractor planning services shall include providing draft documentation and technical input to documentation for assessments, plans, system implementations and architectures, and engineering designs related to new, evolving, and existing C4 systems. At the direction of the Government, the Contractor shall conduct and/or participate in strategic planning, studies, and evaluations to provide resource requirements, present recommended solutions, determine labor and tools estimates, and plan/refine schedules. The Contractor's effort shall include:

- Providing technical studies, reviewing plans, evaluating state of the technologies prior to fielding of new releases or systems
- Reviewing C4 plans and policies and providing observations and questions for consolidated responses
- Researching and coordinating technical issues and requirements and drafting new and updated policy governing technical issues
- Providing technical analyses and draft reports of C4 system tests, assessments, and architectures
- Participating in meetings as required by the Government to include attending conferences; technical interchange seminars; interoperability meetings; and other briefings related to integration, migration, and maintenance of C2, coalition, and bi-lateral system architectures
- Performing analysis, providing recommendations, and preparing planning documentation as directed by the Government for approval to transition current services into the JIE
- Planning large-scale systems and projects through vendor comparison and cost studies and providing input to policy level discussions regarding standards and budget constraints

C.5.2.2.24.2. ENGINEERING AND IMPLEMENTATION

Based upon the outcome of Capability Planning and the Requirements Analysis, the Contractor shall provide emerging communications and information technology engineering support and technical solutions to improve overall service delivery to include customer support, network and system support, IT services, unified communications, storage, etc. The Contractor shall be required to design and build solutions for a wide range of IT projects ranging from the single product level to complex, large-scale, and/or enterprise-type projects. In addition, as services and technologies evolve, new software and hardware will need to be incorporated into the existing baseline as determined by the applicable Government agent. Finally, new security measures will be developed, issued, and require implementation

therefore need to be integrated into existing baselines. To meet these requirements, the Contractor shall:

- Test and evaluate commercial-off-the-shelf applications, Government-off-the-shelf applications and hardware for integration into the C4 networks
- Ensure compatibility with current baseline, resolving conflicts as they arise
- Apply appropriate security measures (STIGs, IAVMs, Tasking Order Compliance, etc.) to lock down the application/hardware
- Develop deployment procedures (i.e. package software, installation instructions, etc.)
- Conduct Cyber Security review and sign-off acceptability prior to deployment
- Test and evaluate Cyber Security-directed patches for compatibility with the current baseline and resolve any conflicts prior to deployment
- Provide design and engineering support for new network and system implementations and upgrades to include hardware, software, projection systems, video switching hardware, video teleconferencing, and other systems to meet project requirements
- Develop solutions to migrate services from the current environment to the CCMD approved solution
- Identify training needs and recommend solutions for Government approval
- Provide effective technical solutions to complex problems to include Tier 3 troubleshooting of incidents or problems when requested

C.5.2.2.24.3. MIGRATION AND TRANSITION

The Contractor shall provide migration and/or transition support to implement approved, engineered solutions into the designated CCMD solution. Migration and transition may range anywhere from moving a service to a new provider such as Enterprise E-mail, moving to a new or upgraded application or hardware, operating system upgrades, life cycle replacement, etc. The Contractor shall plan, document, and lead the transition of all system and network devices, including security devices, from the engineering team to the O&M team. For actual implementation and O&M, the team may or may not be the Contractor's personnel. The Contractor shall:

- Draft documentation to include installation instructions and configuration drawings and diagrams for the implementation and O&M team
- Provide over-the-shoulder assistance when necessary to the implementation team
- Provide knowledge transfer on the new technology to the O&M team
- Perform Quality Assurance checks and/or Acceptance Testing as identified in the Project Plan and directed by the Government.
- Review as-built documentation for accuracy and potential problems

The Contractor may be required to use existing O&M personnel and/or surge personnel in order to implement the engineered solution.

C.5.2.2.25. PROJECT MANAGEMENT SUPPORT

The Contractor shall provide project management services pertaining to IT Services and the supporting IT infrastructure in support of the requirements of the PWS. The Contractor shall follow the PMBOK, as well as industry best practices.

C.5.2.2.25.1. INITIATION AND PLANNING

The Contractor shall:

- Conduct site surveys in garrison or at deployed locations to capture and validate site specific requirements and conditions to plan and design the project.
- Document appropriate project justification (e.g. technical studies, reviewing plans, analysis of alternatives, business case analysis, cost benefit analysis, and evaluation of related technologies) prior to project commencement. The Contractor shall receive Government approval for project commencement, to include the approval of project justification documentation, and will follow CCMD governance policies and procedures.
- Develop a Project Charter for Government approval.
- Develop project documentation for Government approval in accordance with DoD and CCMD policies and governance boards, and standards, aligned with the PMBOK framework. Example project documents include project plans, work breakdown structures, schedules and milestones, engineering designs, security assessments, System Security Plans, product specifications, engineering workforce capacity estimates, training needs and recommended solutions for both the IT service provider and end user, the approach for procurement and shipping of equipment, and a migration plan for transition to IT operations.
- Establish required baselines (scope, schedule, budget) and ensure any changes to the baseline go through established change management process.
- Create Work Breakdown Structure (WBS) and establish milestones to provide structured vision of what has to be delivered and if the project follows established baselines.

C.5.2.2.25.2. EXECUTION

The Contractor shall:

- Manage the procurement of equipment, software, and other project related items, as directed.
- Perform integration, installation, and final configuration of project components or services.
- Manage the testing and evaluation of project components for security, compatibility, and interoperability with the current baseline prior to integration into the C4 networks.
- Implement approved migration plan to transition to IT operations.
- Update project documentation. Create new documentation as required.
- Implement training and knowledge transfer as part of turnover activities.
- Perform Acceptance Testing as identified in the Project Plan and as directed by the Government.

C.5.2.2.25.3. MONITORING AND CONTROL

The Contractor shall:

- Manage project requirements and schedules. Document changes to requirements and schedules IAW CCMD Governance.
- Track project deliverables and materials to facilitate completion of the work, within the established timeline, budget, scope, and agreed quality standards. Report on resource conflicts, if applicable.
- Report project status to stakeholders and government leads based on established timelines. Project status reports shall include deliverables, schedule/milestones, outstanding issues, project risks, and additional resource requirements.

C.5.2.2.25.4. CLOSEOUT

The Contractor shall:

- Prepare project closure documentation by logging project completion, providing all project documentation, and reporting results IAW CCMD Procedures. The Government shall approve project closure.
- Provide un-compiled source code, when required.
- Develop project lessons learned to be included in the CCMD Project Lessons Learned Library (currently CCMDs use MS Project Server).
- Establish, update, and maintain authoritative library for CCMD Project Lessons Learned IAW CCMD Procedures.

C.5.2.2.26. LOGISTICS MANAGEMENT

C.5.2.2.26.1. PURCHASING

The Contractor shall purchase communications and IT equipment and materials in accordance with the GSA Alliant 2 GWAC. All purchases shall be approved by the GSA COR consistent with DoD and Army Acquisition Policies, e.g., the DoD Enterprise License Agreement whenever possible. The Tools CLIN is anticipated for the purchase of communications and IT assets to update, maintain, establish or enable sustained communications and computing capabilities for the technical environments that are covered under the scope of this Task Order. Purchases are expected to encompass hardware to include peripherals and expendable supplies; software to include software assurance/maintenance and subscriptions; and professional services.

The Contractor shall ensure that all communications and IT hardware provided has the most cost-effective warranty or support package available from the vendor/manufacturer. In most cases, this coverage should be for parts, repair and return, or remote services vice on-site warranty or support coverage.

Copies of all purchasing invoices for all property book type items procured under this Task Order shall be submitted to the appropriate CCMD or Installation Property Book Office.

C.5.2.2.26.2. SUPPLY CHAIN RISK MANAGEMENT

Supply Chain Risk Management (SCRM) is a systematic process for managing supply chain risk by identifying susceptibilities, vulnerabilities and threats throughout the supply chain and developing mitigation strategies to combat those threats whether presented by the supplier, the supplied product and its subcomponents, or the supply chain.

This task order is subject to the Federal SCRM policies and regulations including the Defense Federal Acquisition Regulation Supplement (DFARS) 252.239-7017 Notice of Supply Chain Risk, DFARS 252.239-7018 Supply Chain Risk, DoD Instruction 5200.44 Protection of Mission Critical Functions to Achieve Trusted Systems and Networks, Section 806 of the FY2011 NDAA Requirements for Information Relating to Supply Chain Risk, and internal DISA SCRM Processes and Procedures.

The contractor shall submit a SCRM plan no later than 10 business days after contract award that describes how the contractor will reduce and mitigate Supply Chain Risk using the security controls outlined below (further described in CNSSI 1253, Appendix D and NIST SP 800-53), as applicable to the task order.

C.5.2.2.26.3. PROPERTY BOOK

The Contractor shall perform as a Property Book Hand Receipt Holder or a sub-hand receipt holder at the discretion of the Installation Property Book Office and pursuant to their guidance. If assigned, the Contractor shall follow all procedures as identify by AR 735-5 Property in addition to any local instructions. Additionally, Contractor employees may be directed to sign temporary hand receipts for property issued for their use. Regardless of whether the contractor is a prime, sub, or temporary hand receipt holder, the Government may only assign them property under their control. This control is not just limited to physical control but also electronic control such as IT equipment in the TR rooms which the Contractor should know when and if it goes missing.

C.5.2.2.26.4. CONFIGURATION MANAGEMENT

The Contractor shall develop Configuration Management Plan(s), processes, and procedures to manage the supported networks and systems. The plan(s) shall complement and work in concert with the client's Configuration Management Plan should one exist. Separate plans for AFRICOM and EUCOM may be required. The plan(s) shall be submitted for approval of the Government. The Configuration Management Plan may be merged with the Asset Management Plan to become the Asset and Configuration Management Plan (ACMP) at the discretion of the Contractor.

Key to the Configuration Management Plan is the Configuration Management Database (CMDB). The Government anticipates that separate databases may be needed on each network to allow for the use of automated tools. The CMDB shall contain configuration data for all equipment on the network which has an IP or MAC address. In addition, the CMDB shall be the repository for approved baselines (i.e OS, desktop, etc) and the Approved Product List both software and hardware.

The Configuration Management Plan shall identify configuration data to be entered into the CMDB, as a minimum it shall consist of:

- Type (workstation, Laptop, Printer, Server…etc)
- Make and Model
- Serial Number
- Active Directory Name

The Contractor shall work directly with technical personnel to gather sufficient data to populate and maintain the CMDB. Problems obtaining required information from Government entities or other contractors shall be reported to the Government for resolution.

C.5.2.2.26.5. ASSET MANAGEMENT

The Contractor shall develop Asset Management Plan(s), processes, and procedures to manage configuration items listed in the CMDB as well as all spare property book items and hardware, software, maintenance agreements, and expendable supplies under their control. As stated previously, the plan may be combined with the Configuration Management Plan to become the ACMP.

Key to the Asset Management Plan is the Asset Management Database (AMDB), the Governments requires a single, authoritative AMDB, maintained on NIPRNet for each major client – AFRICOM, EUCOM, and CJTF-HOA. *(Note: The Contractor may use additional databases provided they feed into the single, authoritative AMDB.)* The Asset Management Plan shall identify what items are to be tracked and how. The AMDB shall consist of the following attributes:

- Type (workstation, Laptop, Printer, Server…etc)
- Make and Model
- Serial Number
- Property Book Item
- Serial Number Controlled
- License
- Maintenance Agreement (Software or Hardware)
- Provenance (if available)
- Warranty Information

If in use then:

- Network Supported
- Location (bldg. and room desired, but if unavailable Caserne or City, Country)

C.5.2.2.26.6. SUBSCRIPTION MANAGEMENT SERVICES (HARDWARE AND SOFTWARE MAINTENANCE)

The Asset Management Plan shall identify specific processes and procedures to be used to manage the client's hardware and software maintenance agreements. The Contractor shall:

- Maintain use the AMDB to record pertinent attributes from all maintenance agreements. These attributes shall include (at a minimum) product name, manufacturer, quantity, items covered, cost, purchase order/contract, primary client organization, and period of performance
- Notify the Client at least 90-days and not to exceed 120 days prior expiration
- Make best value recommendations about the need to renew agreements
- Determine the most cost effective approach to renew the agreements whenever possible consider co-terming similar agreements into a single order
- Follow purchasing processes and procedures to renew when directed by the client
- Assist with "true-ups" of agreements managed under DoD JELAs (i.e. Microsoft, Cisco…etc)

C.5.2.2.26.7. LIFE CYCLE MANAGEMENT

The Contractor shall perform Life Cycle Management functions for hardware items for which they have maintenance responsibilities. Life Cycle Management begins with defining the criteria to be used to determine when equipment requires replacement. Then, that criteria shall be used to identifywhat needs to be replaced and when. Life Cycle Management functions, processes, and procedures shall be defined in the Asset Management Plan. For equipment maintained by the Contractor, the Contractor shall:

- Recommend to the client Life Cycle Replacement (LCR) criteria based upon industry standards, manufacturer end-of-life and end-of-support notices, and Government guidance for each hardware group (e.g. desktops, laptops, printers, DVTC, etc.) or technology in use. The LCR criteria shall be reviewed annually and any changes presented to the client for approval.
- Recommend candidate equipment to the client for lifecycle replacement semi-annually or upon Government request. The recommendation shall identity the specific make/model needing LCR, approximate quantity broken out by network supported, purchase dates or age of the item, approximate replacement cost, and risk assessment of continued usage
- Upon approval by the Government proceed with procurement, integration, project management and release management processes as identified elsewhere in the PWS

C.5.2.2.26.8. WAREHOUSE MANAGEMENT AND OTHER ASSOCIATED SERVICES

The Contractor shall maintain each client's inventory of spare equipment to include Property Book items and other IT supplies such as operating stock and expendable supplies. The Contractor shall:

- Perform receiving functions for all items procured under this contract
- Perform storage, distribution, and turn-in functions for all items identified in the AMDB
- Perform staging and distribution as required to support project work
- Ensure stock on hand is used or programmed to be used prior to purchasing additional items
- Identify and report to the Government equipment that is either lost or damaged beyond economical repair
- When directed, demilitarize and dispose of HW and SW in accordance with DOD guidance
- Identify and report to the Government any excess, lost, damaged, or end of life equipment
- Track and account for storage media (e.g. hard drives, backup tapes) that process and store NATO SECRET information in accordance C-M (2002)49, "NATO Security Policy".

C.5.2.2.27. THEATER SECURITY COOPERATION MANAGEMENT INFORMATION SYSTEM (TSCMIS) SUPPORT

C.5.2.2.27.1. STRATEGIC INFORMATION SYSTEMS SUPPORT

The Contractor shall function as the Database Administrator (DBA), Systems Programmer, and Program Support Specialist for both United States Africa Command (AFRICOM) and United States European Command (EUCOM) for Combatant Command-developed Strategic Information Systems.

The DBA and Systems Programmer duties include importing/exporting data either from or to the Global Theater Security Cooperation Management Information System (G-TSCMIS), Overseas Humanitarian Assistance Shared Information System (OHASIS), Security Assistance Network (SANWeb), Security Force Assistance Common Operating Picture (SFA COP), Joint Training Information Management System (JTIMS), Joint Capabilities Requirements Manager (JCRM) and like databases. Additionally, the Contractor shall troubleshoot database connection issues and building maintenance schemes. Systems Programmer duties shall include ensuring the ability to publish and pull Theater Security Cooperation information from the G-TSCMIS Enterprise Messaging Bus or other prescribed means/methods of information transfer.

The Contactor shall provide Operation Management subject matter expertise, implementation of authorized changes and maintenance of all Command systems that refine and enhance the functionality of these systems. In doing this, the Contractor shall conform to the priorities and timelines established by the functional requirements of user communities as prioritized by members of the respective CCMD systems' program managers. The Contractor shall ensure compliance with the Configuration Control Board for changes against the baseline system. The Contractor shall also facilitate the operation of the system remotely to other sub-EUCOM/-AFRICOM organizations as determined by the respective functional users (i.e., ECJ5 and ACJ5) and authorized by ECJ6/ACJ6 staff. In particular this includes facilitating access by CCMD Embassy Team personnel to systems hosted on Patch Barracks or Kelley Barracks, both within and outside the Commands' NIPR and SIPR portals.

The Contractor shall further maintain, sustain and ensure IA compliance for current EUCOM-/AFRICOM-specific systems (TCP Dashboard, CFR, Conference Registration System/CRS, SAS Plan, Integrated AFRICOM Theater Synchronization System/IATSS, TSC Resources Handbook, CP Writer and TSC Records Exchange/TREX). Taken together, these will provide a comprehensive picture of whole-of-government security cooperation activities to assist decision makers, planners and other users with the ability to view, manage assess and report security cooperation activities and events. To ensure accountability and prioritization of system requirements, the Contractor shall maintain an active database of work requests (i.e., TFS) and provide access to the client. Systems' data is currently used to feed current and future EUCOM/AFRICOM Dashboards, IATSS, and SAS Plan modules. The requirement for these databases to exist and remain operational at EUCOM/AFRICOM is valid until G-TSCMIS can fully assume all of these functions for both CCMDs.

The Program Support Specialist duties include accessing and updating databases, user account management, and the ability to apply specialized technical expertise to perform analysis, testing, and maintenance of systems and products. The Contractor will provide expertise relative to user requirements and develop technical reports and system documentation in Microsoft Office Suite (Word, Power Point, Excel, and Outlook), and provide training as requested. The Contractor will build and generate custom reports when requested - to include but not limited to reports required by DoD policy or National Defense Authority legislation - and be able to synchronize various databases several times a week. Knowledge of Security Cooperation is preferred.

The Contractor shall produce documentation for software customizations in accordance with industry standards. The documentation shall include, but is not limited to:

- Requirements - Statements that identify attributes, capabilities, characteristics, or qualities of a system. This is the foundation for what will be or has been implemented.
- Architecture/Design - Overview of software. Includes relations to an environment and construction principles to be used in design of software components.
- Technical - Documentation of code, algorithms, interfaces, and APIs.
- End user - Manuals for the end-user, system administrators and support staff.

C.5.2.2.27.2. CCMD STRATEGIC SYSTEMS' ENHANCEMENTS

The Contractor is expected to leverage best practices from support services provided to each CCMD in functional areas such as country plan builder, TSC event tracker and/or strategic assessment frameworks. The Contractor will also advise the systems program managers when systems' inefficiencies or redundancies can be avoided or if there is new technology that should be used or implemented. Further

to that end, the customer may require from the Contractor on a one-time/infrequent basis access to consultative services to perform systems analysis for optimal integration/synchronization across all systems.

Each CCMD has developed databases (TCP Dashboard, CFR, Conference Registration System/CRS, SAS Plan, Integrated AFRICOM Theater Sync System/IATSS, TSC Resources Handbook and TSC Records Exchange/TREX) that meet the CCMD need for tracking, validating, analyzing, and visualizing data. Systems developed shall be able to import from or export to authoritative databases (i.e., Global Theater Security Cooperation Management Information System (G-TSCMIS), Overseas Humanitarian Assistance Shared Information System (OHASIS), Security Assistance Network (SANWeb), Security Force Assistance Common Operating Picture (SFA COP), Joint Training Information Management System (JTIMS), Joint Capabilities Requirements Manager (JCRM) as requested by the client. The needs of the Command will dictate the desired capabilities and system requirements/development. The contractor team shall maintain, enhance, and manage capabilities and subsequent applications.

The Contractor will provide the client up-to-date timelines and weekly progress reports to ensure timely release and communication. Additionally, the Contractor will meet with the client and system stakeholders to discuss and develop application requirements and modifications weekly or as needed.

The contractor shall also provide Quality Assurance (QA) support for all maintained web applications, through both regular prototype demonstrations and formalized system acceptance testing between CCMD system owners and the TSC development team.

C.5.2.2.27.3. CONTRACTOR SUPPORT CRITERIA

The Contractor shall provide sufficient personnel to adequately support all operations, maintenance and enhancement workload requirements for the respective CCMD systems (e.g., TCP Dashboard, CFR, Conference Registration System/CRS, SAS Plan, Integrated AFRICOM Theater Sync System/IATSS, TSC Resources Handbook and TSC Records Exchange/TREX). Past experience supporting these systems has demonstrated an annual work load effort as detailed in the attached matrix.

The Contractor must also ensure that a physical proximity exists between supporting personnel and the CCMDs. This is necessary due to a dynamic business environment with business processes that rely on routine (multi-times weekly) and sometimes spontaneous face-to-face meetings with systems' program managers for requirement clarification, question-and-answer sessions with software engineers and to validate various use case scenarios as development progresses.

As many systems' users are located in U.S. Embassies across Africa and Europe, trouble tickets (i.e., system/network outage) from the field require an expeditious response from the systems support team, sometimes working in coordination with local network administrators.

Workload for TSC System Applications						
NIPR Current O&M Projects						
Application	Version	Status	POC	Command	Avg Trouble Tickets Per Year	Avg Enhancements Per Yr
Concept Funding Request (CFR)	2.x	O&M	David Zimmerman	USEUCOM/ECJ5	50	150
TSC Resource Handbook	1.x	O&M	David Zimmerman	USEUCOM/ECJ5	2	60
Conference Registeration Site (CRS)	1.x	O&M	David Zimmerman	USEUCOM/ECJ5	10	65
Country Plan Writer (CPWriter)	1.x	O&M	David Zimmerman	USEUCOM/ECJ5	10	25
SIPR Current O&M Projects						
Application	Version	Status	POC	Command	Avg Trouble Tickets Per Year	Avg Enhancements Per Yr
TREX	1.x	O&M	David Zimmerman	USEUCOM/ECJ5	5	20
TREX Data Management	1.x	O&M	David Zimmerman	USEUCOM/ECJ5	5	5
SAS Plan	2.x	O&M	Ted Getchman, CDR	USEUCOM/ECJ5	850	275
TCP Dashboard	1.x	O&M	Rich Holdren	USEUCOM/ECJ7	50	100
IATSS	3.x	O&M	David Hamlet	USAFRICOM/ACJ5	250	600
IATSS	4.x	Current Project	David Hamlet	USAFRICOM/ACJ5	New development estimated 4000 man hours complete in June of 2018	
Data Visualization Tool	1.x	O&M	Ted Getchman, CDR	USEUCOM/ECJ5	10	30
NIPR Future Development						
Application	Version	Status	POC	Command	Estimated Work	
Concept Funding Request (CFR) - Rewrite	3.x	Future Project	David Zimmerman	USEUCOM/ECJ5	3240 - 4320 man hours	
TCP Dashboard - NIPR Version	1.x	Future Project	Rich Holdren	USEUCOM/ECJ7	360 - 540 man hours	
SIPR Future Development						
Application	Version	Status	POC	Command	Estimated Work	
TCP Dashboard - Rewrite	2.x	Future Project	Rich Holdren	USEUCOM/ECJ7	720- 1080 man hours	
Additional O&M Activities						
Activitiy	Avg Time Spent Per Year					
Server Maintenance	400 hours					
System Documentation	300 hours					
Release Documentation	250 hours					
Emergency/Misc Systems' Requests	500 hours					

* Additional O&M Activities are for AFRICOM and EUCOM systems combined. The effort is split 40/60 AFRICOM/EUCOM.

C.5.2.2.28. EUCOM JOINT CYBER CENTER (JCC) – CYBER ANALYTICS SUPPORT

The Contractor shall provide a cyber analytics team to apply cyber analytics expertise to maintain and continually improve EUCOM's existing cyber threat capabilities. The teams' expertise shall provide ongoing improvements to sustain a robuts Cyber Threat Detection and Defense capability for EUCOM and the EUCOM Theater. The scope of this support includes providing the resources (inclusive of labor, software, hardware, and data) to support the fusion of these cyber threat detection and defense capabilities in a way that provides advanced global threat analysis and resolution. This includes the development and enhancement of Roles and Responsibilities; Operating Procedures; Software Development, Integration, and Implementation; Training; and Analysis related to this capability. The Government requires a minimum Level of Effort of five (5) full time equivalents (FTE) performing the functions below:

It is expected that Contractor personnel will require:

- Top Secret / Sensitive Compartmented Information (TC/SCI) clearance
- IAT Level II (GSEC, Security+, SCNP or SSCP) and CND Analyst (GCIA) certifications to be compliant with DoD 8570.01-M.

The Contractor shall, consistent with technical direction provided by the Government:

- Assist in the enhancement of EUCOM's existing Cyber capabilities.
- This includes:
  - Implementing new organizational and reporting structures as defined by the Government.
  - Providing correlation and analysis of threats and risks across HQ EUCOM internal/external public/open source data.

  - Identifying hostile threat methodologies, attack vectors, and activity of interest.
  - Providing focused operations/threat analysis on known intrusion sets (including, but not limited to, identifying new attack methods and vulnerabilities exploited).
  - Discovering, tracking, reporting, and fusing global network events of interest utilizing cyber intelligence analysis data and methods.
- Support training and knowledge transfer requirements by delivering training on Cyber threat topics and situation and conducting knowledge transfer on Cyber related topics.
- Apply Cyber Subject Matter Expertise (SME) in adversarial methodologies in the Cyber domain and participate in Operational Planning Teams (OPTs) to include support for Tier 1 and table-top exercises
- Examine and recommend industry best practices for capture and use by EUCOM to enable greater inclusion into USG cyberspace Operations, Activities and Actions occurring within the EUCOM AOR to increase cyber analytics and threat sharing across the globe.
- Examine and develop adversarial trend analysis outside of standard DODIN network purview (i.e. energy, political, financial) to drive predictive analysis of cyber threat actors across all lines of effort in EUCOM AOR.
- Provide detailed back-office analysis and technical support to Joint "hunt forward" Operations
- Develop and administer an Advanced Persistent Threat Course for US and Foreign personnel.
- Provide cyber analytic and technical expertise NATO Allies and other US Partners to support EUCOM's Cyber Security Cooperation efforts throughout the AOR consistent with the technical direction and as authorized by the Government. Activities may include:
  - On-site assistance and training
  - Analysis of allied and partner nation cyber analytics capabilities
  - Supporting EUCOM's efforts to cultivate and build technical relationships and information sharing of Advanced Persistent Threats
  - Participating in conferences and symposiums as presenters and/or workshop leaders
- Plan, develop agenda and curriculum, recommend presenters/speakers, and manage EUCOM's yearly, multiple-day unclassified Cyber Analytics working group spanning USG, Foreign allies, and Corporate partners to facilitate collaboration, information sharing, and technical exchanges.

Specific deliverables associated with the support are expected to include:

- WEEKLY REPORTS - The Contractor shall provide weekly Tip/Threat Summary Reports via email (NIPR, SIPR and/or JWICS) every Friday on world-wide cyber threat occurrences and trends that may affect Blue Force networks in the EUCOM Theater.
- CYBER TIPPERS - The Contractor shall provide cyber tippers as required for any cyber events that could impact Blue Force networks in EUCOM Theater.
- BRIEFINGS - The Contractor shall provide briefings and reports as needed to various entities in the Cyber Center, JFCCC, and EUCOM HQ based on intrusions, events or world-wide actions that could impact Cyber in the EUCOM Theater.
- NETWORK ANALYTICAL REPORTS - The Contractor shall create Network Analytical Reports on large intrusions or events that affect multiple Blue Force Networks in the EUCOM Theater.
- AD HOC REPORTS - The Contractor shall provide briefs for leadership that will be created as requested by the Cyber Center, JFCCC, and/or EUCOM HQ to educate leadership on events, intrusions, and actions taking place in the Cyber Domain.
- SPOT REPORTS - The Contractor shall provide spot Reports on intrusions and events that occurred in the EUCOM Theater and need a quick turnaround to provide information in a serialized manner to various Cyber communities.

C.5.2.3. CONTRACTOR TRAINING

The Contractor must provide and maintain a qualified workforce (see paragraph H.4) therefore in most circumstances training to include the cost associated with it and the time spent doing it is the responsibility of the Contractor or individual employee – not the Government's. However there are circumstances where training (cost, time, or travel) may be charged to the Government. Allowable training includes:

C.5.2.3.1. ORGANIZATION TRAINING

Specific organizational training, normally upon assign to an organization or of a recurring nature, that is required of all personnel (Active Duty, DAC Civilian, or DoD Contractor). *Note: This does not include training that is solely required by the Contractor.*

C.5.2.3.2. ON-THE-JOB TRAINING

An objective of DoD 8570.01-M is to "Implement a formal IA workforce skill development and sustainment process" comprised of among other things OJT. Therefore, while the Contractor is required to provide qualified personnel, this does not mean they know all the systems/tools used or local procedures/processes. In order to meet the objective, the Contractor shall develop and implement a training plan which at a minimum:

- Trains their employees on the local procedures and TTPs used in performance of their duties.
- Trains both IAM and IAT personnel on the specific IA Tools (e.g. ACAS, HBSS) used by the employee in performance
- Identifies how training is to be accomplished (e.g. OJT, CBT, classroom attendance)
- Provides for knowledge augmentation and expansion on a continuous basis as processes, procedures, TTPs, and tools change
- Identifies how and where training is documented for individual contractor employees.

Note: Initial OJT Evaluations are not required as due to contract and TESA requirements for qualified and experienced personnel

C.5.2.3.3. NEW SYSTEMS, APPLICATIONS, OR TOOLS

When a new technology requires support or services by the Contractor, they may request formal training from the Government. The request shall detail the rationale as why it is required, identify how it will be obtained or provided, and how many employees require the training. Every effort shall be made to minimize cost and time but still receive required training. The request shall be made to the COR and/or the Contracting Officer; the client may also be notified at the same time as the COR.

Training shall not be requested for upgrades of existing hardware, systems, operating systems, etc. unless there are extenuating circumstances (i.e. Government implementation comes shortly after product release that places an undue burden on the Contractor). However, should the client offer, the Contractor may take advantage of vacant "seats" provided the Government is not charged labor or travel. The Contractor shall redirect all other client offers of training to the COR

C.5.2.4. PROGRAM MANAGEMENT SUPPORT

The Contractor shall provide program management support under this Task Order. This includes the management and oversight of all activities performed by contractor personnel, including subcontractors/teaming partners, to satisfy the requirements identified in this Performance Work Statement (PWS). The Contractor shall identify a Program Manager (PM) by name, who shall provide

management, direction, administration, quality assurance, and leadership of the execution of this Task Order. The Contractor shall identify Contractor Site Leads and Technical Leads by name, who shall, in concert with the Contractor's PM, provide day-to-day operational level leadership and technical guidance to contractor personnel performing work under this Task Order.

C.5.2.4.1. PROGRAM MANAGEMENT PLAN

The Contractor shall develop and maintain a comprehensive Program Management Plan (PMP) for each client – AFRICOM, EUCOM (including MNIS), CJTF-HOA, ISKM, TSCMIS, and JCC. The Contractor shall submit the plans for Government acceptance within 60 calendar days of the effective date of the Task Order. The plans are living documents; therefore, must be regularly reviewed and updated. The Contractor shall ensure the PMP is accessible electronically and shall be prepared to brief the content to the Government within 3 business days of request.

The plans shall describe the proposed management approach tailored to the requirements and needs of each client. The plan shall consist of several components and smaller plans, not all components are needed for each client. Additionally, some components and smaller plans may not be unique; therefore, they could be utilized for multiple clients. At minimum, the Program Management Plan components shall include:

- Service Strategy Plan
- Service Management Integration Assessment
- Risk Management Plan
- Business Relationship Plan/Communication Plan
- Information Security Management Plan
- Supply Chain Risk Management Plan
- Service Transition Plan
- Asset Management Plan
- Configuration Management Plan
- Change Management Plan
- Training Plan for certification of 8570
- List of deliverable designating frequency and format
- List of Contractor developed TTPs and SOPs
- Quality Control Plan
- Service Operations Plan
- Continual Service Improvement Plan
- Financial Management Plan

C.5.2.4.2. PROJECT ENGINEERING PLAN

The Contractor shall provide a monthly Project Engineering Plan (PEP) for managing backlog of project requests for each stakeholder organization. The monthly Project Engineering Plan shall include status of short-term and long-term projects.

C.5.2.4.3. CONTRACT ACTIVITY AND STATUS MEETINGS

The Contractor Program Manager shall convene a monthly Contract Activity and Status Meeting with the TPOCs, COR, and other government stakeholders. The scheduling for the Contract Activity and Status Meeting will be at a date and time mutually agreeable to the Contractor and the TPOCs/COR. The purpose of this meeting is to ensure all stakeholders are informed of the monthly activity and status report, provide opportunities to identify other activities and establish priorities, and coordinate resolution of identified

problems or opportunities. The Contractor shall provide minutes of these meetings, including attendance, issues discussed, decisions made, and action items assigned, to the COR within five calendar days following the meeting.

The Contractor shall provide the Government real-time access to metrics on communications and information technology support, to include actual statistics, trend analysis and performance measurements and assessments.

C.5.2.4.4. MONTHLY STATUS REPORT (MSR)

The Contractor shall develop and provide a MSR using common office productivity suite applications, by the 15th of each month via electronic mail to the Client Technical Point of Contact (TPOC), designated client representatives, and the COR. Information included in the MSR shall be segregated in accordance with a Government approved format. The MSR shall include the following:

- Activities during reporting period, by task (Include: On-going activities, new activities, activities completed; progress to date on all above mentioned activities). Start each section with a brief description of the task.
- Problems and corrective actions taken. Also include issues or concerns and proposed resolutions to address them.
- Personnel gains, losses and status (security clearance, TESA, etc.).
- Government actions required.
- Schedule (Shows major tasks, milestones, and deliverables; planned and actual start and completion dates for each).
- Summary of Ad-hoc Technical Reports provided.
- Summary of trips taken, conferences attended, etc. Attach trip reports to the MSR for reporting period.
- Accumulated invoiced cost for each CLIN up to the previous month.
- Projected cost of each CLIN for the current month and forecasts through the end of the current performance period.
- Comparison data / monthly performance reports.

C.5.2.4.5. PROGRAM METRICS

The Contractor shall provide the Government with written Monthly Metrics which:

- Provide quantitative measurements which capture and evaluate communications and information technology support, identify trends, and measure performance.
- Serve as a measure of Contractor effectiveness

The Contractor shall work with the Government to identify and incorporate specific measures to include: establishing the targets and acceptable quality levels for specific measures; methods of calculation and manner of collection; and the format for reporting. It is expected that program metrics will evolve from time to time as program needs change and will include performance standards cited in this PWS and other metrics applicable to the scope of services covered under this Task Order.

Note: Reference PWS Attachment J – Performance Requirements Summary for Service Level Agreements.

C.5.2.4.6. TASK ORDER TRANSITION

The incoming and outgoing Contractors shall work together, in collaboration with the Government, to realize Transition-In and Transition-Out Plans to effect a transition that provides for smooth operational turnover which minimizes operational impact to supported organizations.

C.5.2.4.6.1. KICKOFF MEETING

The Contractor shall participate in a Kick-Off Meeting with the Government at a time and place scheduled through the GSA Contracting Officer, or designated representative. The meeting will provide an introduction between the Contractor personnel and Government personnel who will be involved in administration of the Task Order. The meeting will provide the opportunity to discuss task order transition; technical, management, and security considerations; reporting and deliverable submission procedures; travel/tool/ODC approval processes; billing/invoicing procedures, etc. At a minimum, attendees shall include Contractor and GSA key personnel.

C.5.2.4.6.2. TRANSITION-IN PLAN

The Contractor shall prepare, for review and approval of the Government, a Transition-In Plan that includes a schedule depicting the transition activities and milestones for accomplishing the Task Order transition.

The Contractor shall perform the following activities during the transition-in period:

- Perform joint inventories and inspections of all furnished facilities and property with the government and outgoing contractor.
- Perform joint identification and inventory of all contractor maintained classified data, equipment and devices relevant to the performance of the task order, to ensure that proper accountability and chain of custody is maintained for all COMSEC sensitive items.
- Develop and validate a comprehensive communications and IT supported equipment list with the government and outgoing contractor.
- Coordinate with the government to validate or establish maintenance priorities for supported equipment.
- Establish procedures with the outgoing contractor to transition operations, maintenance, and logistics functions while maintaining an uninterrupted continuity of services without a degradation of service. This includes defining processes for turnover of system administration, accounts, privileges, and access.
- It is anticipated that weekly status meetings with all pertinent stakeholders at a mutually agreed upon day and time will be conducted.

C.5.2.4.6.3. TRANSITION-OUT PLAN

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 develop, document, and provide a Transition-Out plan NLT 180 days prior to the Task Order end date or earlier if directed by the Government. 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:

- Project management processes.
- DESMF process and procedures and associated Charters

- Points of contacts within the Government and with those external to include contractors, subcontractors, suppliers, other Government officials
- Location of technical and project management documentation.
- Status of ongoing technical initiatives.
- Transition of personnel.
- Plan to establish and maintain effective communication with the incoming contractor/Government personnel for the period of the transition.
- Inventory, inspection and transfer of IT software and hardware, licenses, and warranties.
- 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.
- Technical artifacts and configuration baselines.
- Elevated system privileges.
- Operations, maintenance, helpdesk, engineering and logistics functions.
- Maintenance priorities for supported equipment.

C.5.2.5. DELIVERABLES

The following schedule of milestones and deliverable submission dates will be used by the COR to monitor timely progress under this Task Order.

The following abbreviations are used in this schedule:

- N/A: Not Applicable
- IAW: In accordance with
- NLT: No later than
- TOA: Task Order Award
- All references to days imply workdays, unless otherwise noted

DELIVERABLES	DUE DATE / PLANNED COMPLETION DATE
Program Management Plan (PMP) inclusive of: • Quality Control Plan • Risk Management Plan • Communications and Change Management processes	Draft within 10 calendar days following the Kickoff Meeting Final within 10 workdays after Government comment; Updates, as required during performance
Network Documentation	IAW PMP
Maintenance Management Plan	IAW PMP
Supported Equipment List	IAW PMP
Maintenance Actions Summary Report	IAW PMP
On-Call Rosters	IAW PMP
Access Control Lists	IAW PMP

DELIVERABLES	DUE DATE / PLANNED COMPLETION DATE
Backup and Recovery Plan	IAW PMP
COOP Exercise Reports	Annual
COOP Exercise Plan	30 calendar days prior to the anticipated start date of the exercise
VTC Usage Report	IAW PMP
Certification and Accreditation Documentation	IAW PMP
Security Event Logs	IAW PMP
Information Assurance SOP/TTPs	IAW PMP
IA Compliancy Reports	Weekly, Every Wednesday
Plan of Action and Milestones (POA&M)	IAW PMP
Engineering Assessments	IAW PMP
System Documentation	IAW PMP
Preliminary Studies	IAW PMP
Strategic Planning Studies	IAW PMP
Estimates and Schedules	IAW PMP
Technical Studies	IAW PMP
Draft Technical Policy	IAW PMP
Network Architecture Plan	IAW PMP
C4 Network Systems Documentation	IAW PMP
C4 Systems Architecture Documentation • Draft C4 Systems Architecture Technical Product • Final C4 Systems Architecture Technical Product	IAW PMP, Quarterly Updates Final Due 10 workdays after Government comment
C4 System Tests, Assessments, and Architecture Reports	IAW PMP
Technical Implementation Instructions	IAW PMP
Migration/Transition Planning Documentation	IAW PMP
AFRICOM Engineering documentation: • Project Charter • Implementation Plan • Engineering Design Plan • Requirements Baseline Document • Test Plan • Test Results • Project CONOPS	IAW PMP
EUCOM Engineering documentation: • Requirements Document • Engineering Reviews	IAW PMP

DELIVERABLES	DUE DATE / PLANNED COMPLETION DATE
• Implementation Plan • Test Plan • Test Results • Migration/Transition Documentation	
Project Management Plans and required PMBOK-aligned deliverables	Draft within 10 calendar days following each project Kickoff Meeting Final within 10 workdays after Government comment; Updates, as required during performance
• SME Support Activity Report • Audit report	IAW PMP
Network Configuration Documentation	IAW PMP
Configuration Control Board (CCB) Minutes	IAW PMP
Property Accountability Records	IAW PMP
Sub-Hand Receipts	IAW PMP
Purchasing Invoices	IAW PMP
Classified Data, Equipment and Devices Inventory	IAW PMP
Communications & IT Refresh/Integration Milestone Plan	Quarterly Updates
PMP Briefs	On 3 business days notice
Project Engineering Plan	Monthly
Contract Activity and Status Meetings Minutes	Within 5 calendar days following the monthly meeting
Monthly Status Report (MSR)	By the 15th of each month
Metrics Report	Monthly to coincide with submission of Monthly Status Report
Trip Reports	IAW PMP
Technical Expert Status Accreditation (TESA) and Technical Representative (TR) Documentation	IAW PMP
Contractor Manpower Report	By October 31 of each calendar year
Kick-Off Meeting	Upon Task Order Award, as scheduled by the GSA CO or designated representative
Transition-In Plan	NLT 15 days following the start of the period of

DELIVERABLES	DUE DATE / PLANNED COMPLETION DATE
	performance of the Task Order
Transition-Out Plan	NLT 180 days prior to end of final performance period, or as otherwise directed by the COR

C.6. OPTIONAL SUPPORT SERVICES

C.6.1 OPTIONAL SUPPORT GUIDELINES

The Government reserves the unilateral right to exercise the following optional services. Options will be invoked through award of a Task Order modification issued by the Contracting Officer. Options may be invoked, in whole or in part, at the discretion of the Government. The Contractor will be provided 75 days from time of option exercise to staff positions.

At the time of exercising an option, the Government will further definitize requirements, where necessary to:

- Provide technical direction necessary to clearly delineate the extent of support and nature of work to be performed, deliverables and required timeframes, if any.
- Specify technical details about the specific environment (e.g. network, systems, applications, tools) where support is required.
- Identify place(s) of performance.
- Define the business hours in which support is required and specify requirements, if any, for providing 7-days a week, 24-hour coverage or recall during non-business hours.
- Identify required service level(s) and performance standards, if any.
- Specify security clearance requirements.
- Identify specific certification requirements of DoD Manual 8570.01M, Information Assurance Workforce Improvement Program applicable to the option being invoked.

C.6.1.1. POTENTIAL OPTIONAL TASKS

Options described may be invoked to support the CCMDs requirements that fall within the scope of the requirements of this PWS. Optional positions are anticipated to include technical skillsets similar to the labor mix performing mandatory services under this Task Order.

For proposal purposes, the Not-to-Exceed (NTE) value of this unburdened option is **$25,500,000** per year ($16,000,000 Labor, $7,500,000 ODCs, and $2,000,000 ODCs – Education). The value of this option includes labor and ODCs support.

Potential Optional Tasks for both AFRICOM (including CJTF-HOA) and EUCOM are listed below. At the time of executing an option, the Government will provide details of expected functions and roles. The below tasks is a non-exhaustive list; however examples of such support include the following, but are not limited to:

C.6.1.1.1. CJTF-HOA PROJECT INTEGRATION SUPPORT

The CJTF-HOA and Camp Lemonnier consume USAFRICOM provided IT services. The CJTF and Camp required a project integrator to ensure the unique services provided at CJTF-HOA integrate with the enterprise services delivered by USAFRICOM. Time has shown that this unique requirement cannot be met from personnel stationed outside of Camp Lemonnier. The PM Integrator will provide concept, technical, and integration support to ensure enterprise services are consumable from Camp Lemonnier.

C.6.1.1.2. CLOUD SERVICES INTEGRATION

If, as projected, CCMD hosts a cloud service in one of its data centers, the Contractor will be required to analyze which services can be hosted on a cloud infrastructure, understand how service level agreements are measured (given that they do not control the cloud services infrastructure), and provide IT functions and services within this infrastructure to the CCMD. The Contractor will develop a cloud integration plan that the Government will approve prior to beginning any migration of application or data to the proposed cloud service. The plan must include integrated IT Service management with the cloud provider.

C.6.1.1.3. ORGANIC INCIDENT RESPONSE TEAM

It is anticipated that AFRICOM may require the development of an internal security incident response team to orchestrate the full lifecycle of a security incident. At the time of exercising the option the Government will provide details of expected functions and roles. Examples may include a Security Incident Response Manager, Security Analyst, Threat Researchers, and Audit Analyst.

C.6.1.1.4. ENTERPRISE LOGGING PROGRAM FOR COMPLIANCE AUDITS

The Government may require the development of enterprise logging services to collect and ingest any type of log files across the enterprise into a central logging service. These log files will be reformatting without changing their content to ensure that they can be processed and managed to render user knowledge of the logging status. The logs will be held according to published Government requirements.

C.6.1.1.5. C2 COMMON OPERATIONS PICTURE/COMMON INTELLIGENCE PICTURE (COP/CIP)

The Government may require support with architectural analysis, requirements elicitation, and technical development of IT services and presentation services to improve on-demand and near-real time visibility of theater assets and security postures. This COP/CIP would provide status of operational readiness support through the visualization of operational support services configurable by mission profile.

C.6.1.1.6. OUT-OF-BAND (OOB) MANAGEMENT NETWORK FOR CLASSIFIED AND UNCLASSIFIED NETWORKS

The Government may require the development of an Out of Band Network for the secure management of its IT infrastructure, Data Center devices, and Telecommunications Closet endpoints. The Contractor would be to develop the classified OOB followed by an unclassified OOB network. They can use the same infrastructure if it is virtualized and connections can be approved by the Authorizing Official.

C.6.1.1.7. SATELLITE COMMUNICATIONS PLANNER [*EXERCISED FOR AFRICOM*]

The Government requires Satellite Communications (SATCOM) requirements analysis and validation, and planning for military and commercial SATCOM IAW DoD and CCMD Policies and Procedures. In addition, the requirements include Theater Information Management duties, Satellite Database Management duties, and operational support of Super High Frequency (SHF), Ultra High Frequency (UHF), and Global Broadcast System (GBS) resources.

The Contractor shall have knowledge of satellite systems in the Extremely High Frequency (EHF), Super High Frequency (SHF) and Ultra High Frequency (UHF) spectrums. Systems include: Advanced EHF, Military Strategic and Tactical Relay (MILSTAR), Wideband Global SATCOM (WGS), Global Broadcast Service (GBS), Defense Satellite Communications System (DSCS), Wideband Global Satellite (WGS), and Mobile User Objective System (MUOS) programs.

Contractors may be required to be read into ACCM, as appropriate, in order to perform their required job functions supporting operations.

C.6.1.1.7.1. MILITARY SATELLITE COMMUNICATIONS PLANNER [*EXERCISED FOR AFRICOM*]

The Contractor shall provide expert guidance and direction for Satellite Communications (SATCOM) activities that include systems in the Extremely High Frequency (EHF), Super High Frequency (SHF) and Ultra High Frequency (UHF) spectrums within the AOR. Systems include: Advanced EHF, Military Strategic and Tactical Relay (MILSTAR), Wideband Global SATCOM (WGS), Global Broadcast Service (GBS), Defense Satellite Communications System (DSCS), Wideband Global Satellite (WGS), and Mobile User Objective System (MUOS) programs.

The Contractor shall provide technical support, asset management and assignment to national level users within the Executive Branch, DoD, and other Government agencies when setting up communication channels. Users include the President, Vice President, Executive Level Secretaries, Joint Chiefs of Staff, Joint Staff, White House Communications Agency (WHCA), other CCMDs and all war-fighting components assigned to the AOR. The Contractor shall coordinate directly with senior level (O-6, General Officer, and SES level) officials and Action Officers (AOs) to ensure user requirements are being met in a timely and precise manner.

The Contractor shall coordinate operational and programmatic issues with Regional and Functional Combatant Commanders, the SATCOM System Operational Manager (SOM), terminal and control Program Managers from all Services, and other SATCOM System Experts (SSEs). The Contractor shall be responsible for CCMD SATCOM missions as assigned by the Commander, the CCMD and other various entities. This support includes, but is not limited to, the following: Provide an integrated SATCOM management infrastructure responsive to all users - strategic and tactical.

The Contractor shall provide technical and non-technical input to the Joint Staff, regional and functional Combatant Commanders, terminal and control Program Managers from all Services and other SATCOM Systems Experts to oversee the development and integration of all Satellite Communications concepts and systems in the Joint Capabilities Integration Development System (JCIDS), to include: Initial Capabilities Documents (ICDs), Capabilities Development Documents (CDDs), Capabilities Productions Documents (CPDs), Information Support Plans (ISPs), Concept of Operations (CONOPS) and other documents relating to SATCOM.

The Contractor shall provide input to the Joint Staff, Regional and Functional Combatant Commanders and all Services on the use of current SATCOM assets. Additionally, the Contractor shall provide input to the Joint Staff, Regional and Functional Combatant Commanders and all Services on the development, integration, interoperability and eventual deployment of future SATCOM architecture.

The Contractor shall provide input to the Joint Staff, Regional and Functional Combatant Commanders and all Services on matters pertaining to Global SATCOM standards, policies and procedures as well as

Satellite Communications Priorities. The Contractor shall provide input and oversight on the development of theater SATCOM standards, policies and procedures. With the approval of the Government, the Contractor shall implement national level guidance and establish policies for these systems in the AOR.

The Contractor shall serve as the Command's focal point for technical, non-technical, architectural and administrative issues related to SATCOM, both military and civilian. The Contractor shall evaluate emerging technologies in SATCOM, command and control, Position, Navigation and Timing (PNT), and advanced SATCOM technology systems development. The Contractor shall conduct studies and develop policies, for Government approval, involving both long-range and short-range plans of CCMD AOR SATCOM operations and requirements. The Contractor shall initiate actions in response to long-term requirements to establish, upgrade or phase out SATCOM facilities and/or capabilities within the AOR. The Contractor shall recommend requirements and potential solutions to enhance the use and efficiency of these programs to the Joint Staff and other entities, as required.

The Contractor shall represent the CCMD, with the Joint Staff, Regional and Functional COCOMs, as well as Component commands within the AOR.

C.6.1.1.7.2. COMMERCIAL SATELLITE COMMUNICATIONS PLANNER [*EXERCISED FOR AFRICOM*]

The Contractor shall provide expert guidance and direction for the Commercial Satellite Communications (COMSATCOM) activities that encompass systems in the Commercial SHF and UHF spectrum and the GBS programs within the AOR.

The Contractor shall provide technical support, asset management and assignment to national level users within the Executive Branch, DoD, and other Government agencies when setting up communication channels. Users include the President, Vice President, Executive Level Secretaries, Joint Chiefs of Staff, Joint Staff, WHCA, Other CCMDs and all war fighting components assigned to the AOR. The Contractor shall coordinates directly with senior level (O-6, General Officer, and SES level) officials and Action Officers (AOs) to ensure user requirements are being met in a timely and precise manner.

The Contractor shall coordinate operational and programmatic issues with Regional and Functional Combatant Commanders, the SATCOM SOM, terminal and control Program Managers from all Services, and other SSEs. The Contractor shall be responsible for CCMD COMSATCOM missions as assigned by the Commander, the CCMD and other various entities. This support includes, but is not limited to, the following: Provide an integrated COMSATCOM management infrastructure responsive to all users - strategic and tactical.

The Contractor shall provide input to the Joint Staff, Regional and Functional Combatant Commanders and all Services on the use of current COMSATCOM assets. Additionally, the Contractor shall provide input to the Joint Staff, Regional and Functional Combatant Commanders and all Services on the development, integration, interoperability and eventual deployment of future COMSATCOM architecture.

The Contractor shall provide input to the Joint Staff, Regional and Functional Combatant Commanders and all Services on matters pertaining to Global COMSATCOM standards, policies and procedures as well as Satellite Communications Priorities. The Contractor shall provide input and oversight on the development of theater SATCOM standards, policies and procedures. With the approval of the Government, the Contractor shall implement national level guidance and establish policies for these systems in the AOR.

The Contractor shall serve as the Command's focal point for technical, non-technical, architectural and administrative issues related to COMSATCOM. The Contractor shall evaluate emerging technologies in COMSATCOM, command and control, and advanced COMSATCOM technology systems development. The Contractor shall conduct studies and develop policies, for Government approval, involving both long-range and short-range plans of CCMD AOR SATCOM operations and requirements. The Contractor shall initiate actions in response to long-term requirements to establish, upgrade or phase out SATCOM facilities and/or capabilities within the AOR. The Contractor shall recommend requirements and potential solutions to enhance the use and efficiency of these programs to the Joint Staff and other entities, as required.

The Contractor shall represent the CCMD, with the Joint Staff, Regional and Functional COCOMs, as well as Component commands within the AOR.

C.6.1.1.8. SATELLITE DISH INSTALLATION AND MAINTENANCE

The CCMDs have several satellite dishes on various buildings at multiple locations providing satellite services. The Contractor must be able to provide satellite dish lifecycle management when required by Government. This could include SATCOM system installation, construction, operations, replacement, and disposal IAW safety requirements.

C.6.1.1.9. AFRICOM DATA SHARING NETWORK (ADSN) SUPPORT AT CJTF-HOA

The Government may require support for the AFRICOM Data Sharing Network (ADSN) hub and remote site SATCOM terminals (network infrastructure, SATCOM connectivity, ADSN systems, and High Assurance Internet Protocol Encryptors (HAIPE)).

The remote terminals provide tactically deployed users with connectivity to the ADSN data currently stored at CJTF-HOA. The ADSN network will be expanded soon to include a 2nd data center at RAF Molesworth; after this is completed, data may be accessed from either location via the ADSN network. The Contractor will need to troubleshoot the CJTF-HOA side of the terrestrial circuit linking the two sites. Each terminal provides the capability for multiple laptops/VOIPs to access services. The ADSN may be comprised of several terminal variants, operating in the Ku and Ka bands. The hub serves as a downlink site using a Rockwell Collins Deployable Ku band Earth Terminal (DKET).

There are 14 planned remote sites planned with a minimum configuration of two workstations, two VOIP phones, and a printer at each remote site. There are 4 U.S. workstations and 3 VOIP phones at the hub in CJTF-HOA.

C.6.1.1.10. ENTERPRISE CONSOLIDATION PLAN PHASE 1 (AESD SERVICES)

AFRICOM is considering a plan to unify its IT service providers for greater efficiency and effectiveness of IT operational processes. Phase 1 of this plan would be obtaining responsibility of the incident and service desk functions. This option would require the Contractor to evaluate the service desk functions currently being provided by the Army Enterprise Service Desk (AESD) and propose a plan to take over providing those services directly to AFRICOM. This may be a stand-alone service or a service that is combined with EUCOM. The Contractor will highlight pros and cons of each approach in their implementation plan. The proposed plan will develop roles, responsibilities, technical solutions, and IT management process integration. Currently the AESD provides service desk services and some additional services outside the traditional service desk.

C.6.1.1.11. ENTERPRISE CONSOLIDATION PLAN PHASE 2 (AFSSA SERVICES)

AFRICOM is considering a plan to unify its service provider environment to enable IT operational process like Incident Management and Event Management. This phase 2 option would require the contractor to build upon the Phase 1 option of Service Desk consolidation. In this phase the contractor would evaluate all services being provided by the AFRCIOM Signal Support Activity (AFSSA) and propose a plan to take over providing those services. Implementation plan would cover roles, responsibilities, technical solutions and IT management process integration. Currently the AFSSA provides some of the Tier 2 services in the incident management process, some security incident management, server maintenance and desktop support.

C.6.1.1.12. ENTERPRISE CONSOLIDATION PLAN PHASE 3 (RCCE SERVICES)

AFRICOM is considering a plan to unify its IT service providers to enable IT operational process like Incident Management and Event Management. This option would follow phase 2 and include the services provided by the US Army Regional Cyber Center Europe. The Contractor would evaluate all services being provided by the Regional Cyber Center Europe (RCC-E) and propose a plan to take over providing those services and fully implement the full range of DESMF processes. Any Implementation plan would cover roles, responsibilities, technical solutions and IT management process integration. Currently the RCC-E provides some of the enterprise enabling services that AFRICOM is reliant upon.

C.6.1.1.13. ENTERPRISE CONSOLIDATION PLAN PHASE 4 (LAYER 2 AND 3 ACROSS DOMAIN)

AFRICOM is considering a plan to own all aspect of its IT service delivery inside the Joint Regional Security Stack boundaries. This Phase, an architectural evaluation of taking over layer 2 and 3 services could be partially combined with phase 2 and phase 3. The Army runs the network upon which USAFRICOM services traverse inside the USAFRICOM security boundaries. This phase would provide the opportunity to completely separate from Army services and simplify the IT Service model at all layers. The Contractor would provide recommendations and timelines on taking over layer 2 and 3 services as well as necessary COMSEC services to enable USAFRICOM to be the responsible entity of all USAFRICOM provided services.

C.6.1.1.14. MISSION PARTNER GATEWAY SECURITY – EXTENDED (MPGW-X) AND SECURITY SERVICES

The Government may require the development of security services covering the Mission Partner Gateway. Currently JRSS does not provide MPG services and an enterprise solution may prove to be more cost effective and secure in the long run. This solution would evaluate the threat to the Mission Partner Environment (MPE) and develop a recommended solution that includes boarder gateway services. MPGW-X is a projected security capability for MPE networks that mimic JRSS function. For this option, the Contractor is expected to manage and operate MPGW-X suites IAW DoD and CCMD Policies and current architectures and coordinate with external in support of MPGW-X operations and migrations.

C.6.1.1.15. EUCOM TMT

Optional TMT support for EUCOM includes user training, trend analysis (to include timing and status), and support for editing and routing products through the staffing process.

C.6.1.1.16. EXECUTIVE COMMUNICATIONS SUPPORT [*EXERCISED FOR AFRICOM*]

Provide VIPs travelling to locations designated by the Government with on-site support to install, operate, and maintain secure communications up to SECRET. Coordinate with CCMD personnel (such as HQ IT Operations, Configuration Management, and Directorate front offices) and assist with the installation, maintenance, troubleshooting, upgrading, and removal of communication suites within executive

quarters at designated locations. Coordinate and manage CSfC training and track training completion. The Contractor will issue equipment and maintain accountability.

Reference PWS Section C.5.2.1.6. for additional VIP Support requirements.

C.6.1.1.17. COP/CIP MANAGEMENT

The COP is maintained in Global Command and Control System – Joint (GCCS-J), the Department of Defense (DoD) Command and Control (C2) Program of Record (PoR). The COP management team fuses and correlates operations, intelligence, logistics, and sensor data with a variety of overlays, Keyhole Markup Language (KML) files, and other Tactical Decision Aids (TDAs) to form the COP for the USEUCOM and/or USAFRICOM Area of Responsibility (AOR). The COP management team will maintain a presence in the Joint Operations Center (JOC).

C.6.1.1.18. MULTI-ENCLAVE SOLUTIONS

The Contractor will implement multi-enclave client solution that allows access to all CCMD required networks to include ULAN, SLAN, Seagull, BICES, USBICES-X bilats, EBN 1,2, and 3, etc.

C.6.1.1.19. CROSS DOMAIN SOLUTIONS MANAGEMENT

The Contractor will operate the devices owned by the CCMD that provide transfer of information and data between network enclaves in the European theater.

C.6.1.1.20. SUPPORT TO MOLESWORTH AND COOP LOCATIONS

The Government may require dedicated IT Services support to Molesworth, UK and EUCOM COOP location.

C.6.1.1.20.1 SUPPORT TO EUCOM COOP LOCATION [*EXERCISED FOR EUCOM*]

Headquarters United States European Command (HQ USEUCOM) has a requirement to execute the Continuity of Operations Plan (COOP) and activate and operate the IT component with the use of facility located at Site B as outlined in Task C.5.1.7.2 CONTINUITY OF OPERATIONS PLAN (COOP) and C.2.5.6 FUTURE CONSIDERATIONS.

The contractor shall provide continual O&M support to the new infrastructure built in support of AMDA Capability Level 1 at Site A and Site B. The contractor shall maintain a physical presence at both locations.

The contractor shall provide support of operational services as defined in section C.5.2 in accordance with the defined COOP policies and procedures supporting EUCOM's Capability Level 1 (CL-1) for services deployed to both Site A and Site B. In addition, the contractor shall provide support of services required to support replication of services deployed to those sites.

Specifically, the Contractor shall provide comprehensive service and support in the following functions:

- Network Security and Cisco Application Centric Infrastructure (ACI)
    - Support the increase of two Security Stacks at Sites A and B
    - Support Cisco Software Defined Networking – ACI
    - Support routers, switches, firewalls, Cisco Identity Services Engine (ISE), Device Management, Performance Management, Traffic Aggregator, Gigamon, Jump server, Crypto, TACLANE, Virtual Private Network (VPN) Cisco Emergency Communication Kits

Kits (ECKs), On-Demand Computing (ODC), Wide Area Network (WAN) and Network Management.

- Platforms
  - Support Core Services (Active Directory (AD), Domain Name System (DNS), Active Directory Federation Services (AD FS), Dynamic Host Configuration Protocol (DHCP), Web Proxy, Online Certificate Status Protocol (OSCP), Print)
  - Additional servers: 30
- Virtual Desktop Infrastructure (VDI)
  - Support Citrix Application Delivery Controller (ADC), VDI, Wyse Devise Manager, Remote access, StoreFront, Delivery Controllers, Director, License Servers and Provisioning Services
  - Additional Servers: 26
- Cyber
  - Support new Risk Management Framework (RMF), Assured Compliance Assessment Solution (ACAS), Host Based Security System (HBSS), Carbon Black / Bit 9 and Varonis
  - Additional Servers: 32
- VI / Storage
  - Maintain and Support:
    - 384 Virtual Servers
    - 750TB Storage

C.6.1.1.20.2 SUPPORT TO MOLESWORTH [*EXERCISED FOR EUCOM*]

The Government requires dedicated IT Services support to Joint Intelligence Operations Center Europe (JIOCEUR) Analytic Center (JAC) in Molesworth, UK

Background:

EUCOM's existing legacy Unclassified Local Area Network (ULAN) and SIPRNet Local Area Network (SLAN) on RAF Molesworth are spread across 20 buildings on the RAF Molesworth campus. The current SLAN and ULAN architecture are comprised of various network devices (routers, switches, encryption devices and firewalls) located in 22 telecommunications rooms (TRs) within the 20 buildings.

These LANs support 825-850 EUCOM users at 14 buildings across the RAF Molesworth campus. The EUCOM users currently access these networks via thick clients and use legacy DSN unclassified phones (i.e. POTS phones, STEs). The local Air Force Communications Squadron currently provides all voice service.

As part of the JIAC Bridging effort, EUCOM will upgrade the aging ULAN and SLAN to the meet standards in accordance with the latest NETCOM N-ICAN and S-ICAN architecture guidance, which will match the N-ICAN and S-ICAN architecture on Patch Barracks. The installation of the N-ICAN and S-ICAN begins 09 NOV 21 and ends 16 AUG 22.

As part of this effort EUCOM is remediating all 21 of the TRs, which includes electrical, grounding, tempest, and ESS. Work began 6 APR 21 and the only effort remains is the completion of ESS.

Also as part of the JIAC Bridging effort, EUCOM will move to a VDI infrastructure and provide DISA EVoIP services. While EUCOM will remove the majority of the thick clients from the networks, the number EUCOM users remains the same. Once transition to DISA EVoIP services, the local Air Force

Communications Squadron will cease to be the voice service provider to EUCOM users. The cutover to a VDI infrastructure and provide DISA EVoIP services begins 8 DEC 21 and ends in SEP 22.

Within the 14 buildings across the RAF Molesworth campus, EUCOM is responsible for 10 conference rooms and a Watch Floor (See Table 1) at RAF Molesworth. As part of the JIAC Bridging effort EUCOM as also modernizing these conference rooms. The existing AV equipment is nearing the manufacturers' end of support (EOS) and the existing AV system does not meet current EUCOM cybersecurity standards. Once the AV Tech Refresh portion of the JIAC Bridging effort is complete, all 10 of the conference rooms and Watch Floor will match the EUCOM J6 conference room standard. This effort is scheduled to begin installation on 21 SEP 21 and complete on 03 JAN 22.

Table 1: JIOCEUR / JAC Molesworth Conference Rooms and Watch Floor

Current:	B100 VTC & Large Conference Room	B100 R214 VTC & Conference Room	B303 RF16 VTC & Conference Room	B320 R11 VTC & Conference Room	B348 JAC Command VTC & Conference Room	B100 JAC I&W VTC & Conference Room
Future:	B100 R103 VTC/DVTC & Conference Room	B100 R136 VTC & Watch Wall	B314 R10 VTC & Conference Room	B414 R11 VTC & Classroom	B414 R12 VTC & Classroom	

Lastly, EUCOM is developing and deploying a multi-site data center architecture to provide mission data assurance. The objective is to provide a resilient physical infrastructure and IT environment capability for continuity of operations and disaster recovery efforts. The Capability Level 3 (CL3) will provide resilient services to include Virtual Server Infrastructure (VSI) and Virtual Desktop Infrastructure (VDI) for approximately 2,550 potential remote users. The project design is currently underway, with requirements gathering in Q1 of FY22 and design completion 29 APR 22. The procurement and installation is tentatively scheduled to begin Q3 FY22 and complete Q4 FY22.

Requirements:
The contractor is required to provide the following comprehensive customer (end user) support on EUCOM ULAN and SLAN networks at RAF Molesworth – either on site or remotely back at Patch Barracks - as marked on Attachment B – Requirements Alignment Matrix (Attached).

Requirements:

The contractor shall provide the following specific requirements:

- Maintain patch management of thick clients until the installation and migration to thin clients is complete. (Anticipated to occur in the summer of 2022)
- Maintain existing SIPR and NIPR ICAN through decommission (Anticipated to occur in the summer of 2022) and facilitate hand-off of new NIPR and SIPR ICAN infrastructures and assume O&M support following SOVT.
- Continue to provide break/fix support on aged infrastructure. New installations and growth would route through J66 for approval.
- Provide installation and configuration of approved VTC endpoints not in conference rooms

- Operate and maintain 10 conference rooms and Watch Floor following the complete installation and turnover from NIWC. No additional conference rooms will be within scope. O&M includes fix, repair, re-program, and update to maintain overall system security posture and functionality. O&M does not include expanding capabilities or building out additional conference rooms without contract modification.
- Maintain firmware upgrades to VDI endpoints once installed. Integrate VDI endpoints into a locally hosted VDI manager and server infrastructure
- Implement and maintain systems endpoint terminals IAW EUCOM Cyber policy (ISE, HBSS, GPO, Carbon Black).
- Perform Cyber Security scanning and remediation for endpoints.
- Configure new VoIP and VoSIP after initial configuration deployment. Deployment includes physical connectivity and configuration of the phone in the DISA call manager.
- Perform annual COMSEC rekey ISO new S-ICAN infrastructure for approximately 30 additional devices).
- Maintain printers IAW applicable STIGs. Perform firmware upgrades as required in response to CTOs. Integrate printers into larger enterprise strategy.
- Operate and maintain additional (new) security stack and DISA circuits – maintain redundant dynamic routing between Site A and Site C in the event of a failure.

<u>Staff Requirements:</u>

Experience installing/ maintaining;
- Thinklogical Matrix switches
- Cisco telepresence Systems
- Crestron Touch Panel systems
- Basic A/V system wiring

Fiber Optics/Network Cabling installation, Termination, and Testing.
Experience in setting up VTC Bridge calls.
Configuring VTC endpoints
Configuring Cisco call manager
Experience with Cisco Meeting Server bridge calls
Certified Cisco Network Administrator (CCNA) required for management of the LAN

C.6.1.1.21. MPE SUPPORT [*EXERCISED FOR EUCOM*]

The Government may require the delivery of a full suite of IT services to European Battle Networks 1, 2, 3.

The EUCOM Multi-National Information Systems (MNIS) program is significantly expanding its capability to provide coalition networks to support operational requirements for the EUCOM Commander. Through network services managed by Secretary of the Air Force – Administrative Assistant (SAF-AA) – Mission Partner Capability Office (MPCO), EUCOM is tasked to increase its footprint of four networks on the EUCOM campus over the next several years. This tasking will require EUCOM to provide Operations and Maintenance (O&M) support while SAF-AA MPCO hosts and manages the enclaves and data centers and, in certain networks, the Virtual Desktop Infrastructure (VDI) backend servers. Additionally, EUCOM is responsible for two network transports to support Coalition and mission connectivity.

EUCOM requires communications and Information Technology (IT) services in support of the various networks and transports listed below; services consist of the requisite labor to perform the technical, administrative, collaborative and reporting services detailed in Performance Work Statement (PWS) Section C; the Other Direct Costs and Travel as defined in the logistical support annexes, and Tools necessary and ancillary to performance.

- European Command NATO Secret (ECNS)

ECNS is the network used for strategic, non-mission specific communication with NATO and the broader NATO SECRET enterprise. ECNS is connected and federated with the NATO SECRET Wide Area Network (NSWAN) network, allowing voice, video, chat, email, authentication, etc. to occur between the two networks.

During OY2, EUCOM expects there to be approximately 500 users on the network through physical network expansion into five buildings as well as integration into the Defense Intelligence Agency (DIA) Trusted Thin Client solution in SCIF spaces. The engineering and large scale rollout of ECNS is handled through separate contracts but EUCOM is tasked to provide input or feedback during the engineering phases of new capabilities. It is expected that the Identity Services Engine (ISE) will be incorporated during expansion. End user devices will include thin clients (i.e. Dell Wyse), Cisco phones, Cisco Video Teleconferencing (VTC) end points and codecs, fat clients, and printers.

- European Mission Network 3 (EMN3)

EMN3 is a mission and exercise network supporting a “Fight Now” concept with coalition partners. EMN3 is currently supporting about 40 users in five buildings at EUCOM ().

During OY2, EUCOM expects there to be approximately 500 users on the network through physical network expansion into at least buildings 2301T, 2358, 2304, 2307 and 2308 as well as integration into the DIA Trusted Thin Client solution in SCIF spaces. The engineering and large scale rollout of ECNS is handled through separate contracts but EUCOM is tasked to provide input or feedback during the engineering phases of new capabilities. It is expected that the ISE will be incorporated during expansion. End user devices will include thin clients (i.e. Dell Wyse), Cisco phones, Cisco Video Teleconferencing (VTC) end points and codecs, fat clients, and printers.

- European Mission Network 2 (EMN2)

EMN2 is a mission network tied for use in the NATO Response Force. EMN2 is only installed in EUCOM building 2301T with less than five users.

End user devices will include thin clients (i.e. Dell Wyse), Cisco phones, Cisco Video Teleconferencing (VTC) end points and codecs, fat clients, and printers.

- European Mission Network 1 (EMN1)

EMN2 is a mission network tied for use in the NATO Response Force. EMN2 is only installed in EUCOM building 2301T with less than five users.

End user devices will include thin clients (i.e. Dell Wyse), Cisco phones, Cisco Video Teleconferencing (VTC) end points and codecs, fat clients, and printers.

- CENTRIX Over the Internet (COTI)

COTI is a commercial ISP gateway that allows coalition partners to connect to ~~Combined Enterprise Regional Information Exchange – Southwest Asia (CENTRIX-SWA) and~~ CENTRIX-Global Counter-Terrorism Force (GCTF) over commercial internet, supporting about 15 coalition partner connections. COTI includes a firewall, router, and crypto devices.

- EUCOM Common Mission Network Transport (CMNT)

CMNT is the preferred transport network for MPE networks. DISA provides CMNT backhaul, but EUCOM manages the CMNT switches and CMNT Customer Edge (CE) routers locally. CMNT is currently installed in five EUCOM buildings (2358, 2301T, 2304, 2307 and 2308). CMNT will be expanded to include every EUCOM building on Patch Barracks over the next 2-3 years.

The CMNT network generally includes a switch per building and two CMNT CE routers hosted on Patch. Classified networked connect to the CMNT switch via an encryptor. It is expected that the ISE will be incorporated during expansion.

C.6.1.1.21.1 MISSION PARTNER ENVIRONMENT (MPE) SUPPORT (OPTION 1)
Growth of ECNS and EMN3 networks by an additional 500 users each in OY3 to 2,000 users total.

C.6.1.1.21.2 MISSION PARTNER ENVIRONMENT (MPE) SUPPORT (OPTION 2)
Growth of ECNS and EMN3 networks by an additional 500 users each in OY4 to 3,000 users total

C.6.1.1.22. MAINTENANCE OF TACTICAL NODE FOR SERVICE EXTENSION
The Government may be required to maintain the tactical node for the service extension.

C.6.1.1.23. BUSINESS INTELLIGENCE SERVICES
The Government may require Collaboration/KM Engineers skilled in IT related business process engineering with IT expertise to develop automated solutions/dashboards. Services will be in support of key IT business processes with the objectives and priorities as defined by the CCMD TPOC. The planned outcomes are to enable:

- Access to expertise and authoritative information from an integrated knowledge environment
- Effective flow of knowledge within CCMD J6 and the other directorates
- CCMD J6 to become a learning organization employing optimized processes

C.6.1.1.24. EUCOM SSO DATABASE UPGRADE [*EXERCISED*]
The Government may require the Special Security Office (SSO) database to be upgraded to standard technologies. The Contractor will be expected to validate existing application requirements and gather new requirements; rewrite/upgrade existing application; integrate the new application into the production environment; and migrate current data to the application. Example deliverables include a Project Plan, an Application Requirements Document (requires Gov't sign-off), and an Application Source Document (code, data mapping, schema). The Contractor will also be expected to manage and operate the system. Example tasks include database administration, patching and compliance actions, backups, and account management.

EUCOM Special Security Office (SSO) is upgrading its database and web frontend to provide enhanced capabilities to improve interdepartmental processes and workflows. The Contractor shall provide singular support to EUCOM SSO, with no alternate projects and maybe part of a team providing development,

implementation, and maintenance support for sub components, associated staff elements, and organizations (EUCOM, SHAPE SSG and JAC Molesworth). The supported commands require development support services for the continued enhancement, operation, and maintenance of the EUCOM SSO database and web frontend serving the EUCOM SSO.

SUPPORT REQUIREMENTS

The Contractor shall provide technical services in support of this effort that include, but are not limited to, ASP.NET development; database maintenance/modifications; software/database updates that implement cyber-security updates identified by vulnerability scanners and/or as required by applicable Security Technical Implementation Guides (STIG); database and system backups; account management; as well as, provide ongoing technical support during the entire service lifecycle. The contractor is expected to work with ECJ24-SSO, SHAPE SSG and JAC personnel to gather and document new requirements; rewrite/upgrade existing application; integrate the new application into the production environment; and migrate current data to the application. The Contractor will also be expected to develop, test/launch, manage and operate the system.

The Contractor must be able to develop, install, test, debug, document Web-based applications, diagnose and fix issues with web applications, and ensure web server and application server technical performance meets customer requirements and complies with all mandatory cyber-security requirements (exceptions may be documented and approved by the customer). Primary duties include development, implementation, and maintenance of ASP.NET frontend and SQL backend database, as well as assisting on modernization projects to incorporate legacy applications/functions into the new SSO database capability (e.g. import data brought up from external sources such as JPAS, DISS, EUCOM SIPR shared drives & shareportal – Incident Reports, Foreign Contacts, Foreign Travel, DEROG, Courier Orders, foreign nationals access to SCIF, personnel security records, security forms/templates, reports, badge access etc.).

DELIVERABLES

The contractor shall provide the following deliverables during the design and installation phases of the project:

- Project Management Plan:
    - The report must allow the reader to develop a clear and concise understanding of project tasks and subtasks including task dependencies. Dates must be defined for each task/milestone.

  Weekly In-Progress Review (IPR) briefings:
    - Briefing must include an overall project status and review of project timelines, any changes to project schedule, work accomplished since last IPR, upcoming work planned, issues that may impact project delivery timeline, and any issues that require government intervention.
- Weekly In-Progress Review (IPR) briefings:
    - Briefings must include an overall project status and review of project timelines, any changes to project schedule, work accomplished since last IPR, upcoming work planned, issues that may impact project delivery timeline, and any issues that require government intervention.
- Application Requirements Document (requires Gov't sign-off)
- Application Source Document (code, data mapping, schema)
- Technical Solutions Documentation

- Documentation must provide high-level specifications regarding technical requirements of the project, the solution design process flow, data flow diagram describing the recommended technical solution/s, list of activities, best practices guidelines, and integration/deployment scenario including supporting materials. Documentation must be written to provide a clear and concise understanding of technical issues.

- Deployment and Rollback plan
  - Prior to deploying changes in the production environment, a deployment plan will be provided outlining the planned changed to the environment, the deployment strategy, a rollback plan, services that will be impacted during the change, and any expected downtime required to implement the change.

PERIOD OF PERFORMANCE

The design, implementation and migration of the system shall be performed by the Contractor with on-going maintenance and operations enduring through the remainder of the task order.

ADDITIONAL REQUIREMENTS

Required Skills:

- 6+ years' experience developing web applications using C# ASP.NET / ASP.NET Core
- Can develop interactive browser based applications using JavaScript / Typescript / Angular
- Intermediate level proficiency with CSS3/Bootstrap
- Experience with one or more of the following programming languages (or similar) are required
  - Programming in HTML5 w/ JavaScript and CSS3
  - Programming in C#
  - Developing ASP.NET MVC Web Applications
  - Developing Microsoft Azure and Web Services
  - Software Testing with Visual Studio
  - HTML5 Application Development Fundamentals
- CompTIA Security+ (or other certification IAW DoD 8570.1 Technical Level II)

Security:

- Candidates must have an active Secret Clearance with the ability to obtain and maintain a Top Secret Level Clearance (Note: If possible the candidate must have the ability to obtain and maintain TS/SCI to have access to the EUCOM SSO SCIFs. There will be seating available in the EUCOM SSO for contractor to complete the project.)

C.6.1.1.25. WIRELESS NETWORK MANAGEMENT

The Government may require the design, development, installation, configuration, operation, and management of an unclassified wireless network on select campuses or buildings.

C.6.1.1.26. NETWORK CONTROL CENTER SUPPORT [*EXERCISED FOR AFRICOM*]

The Contractor will provide 24/7/365 support to the CCMD Network Control Center to perform specific functions, as directed, IAW CCMD Procedures. Examples of tasks include: monitoring of operational system and network status, initial triage and troubleshooting of events and incidents, coordination for

escalated troubleshooting or support of events or incidents, ASI management, and tracking of cyber security incidents.

The Contractor will provide support during core duty hours to the CCMD Network Control Center to perform specific functions, as directed, IAW CCMD Procedures. Examples of tasks include: management, coordination, and tracking of DoD Orders and Directives, for example, TASKORDs, OPORDs.

- The Contractor will develop and document recommendations for CCMD Network Control Center processes, technology, or configuration improvements IAW CCMD Procedures.
- The Contractor will develop and document After Action Reports (AAR), as directed, and after contingency operations, and named exercises.
- The Contractor will provide Network Control Center Services in a Government designated location. It is expected that this location will be in Stuttgart, Germany.
- The Contractor will represent the CCMD Network Control Center as functional Subject Matter Experts (SME) in CCMD Governance boards IAW CCMD Policies.
- The Contractor will facilitate CCMD Network Control Center Network Operations Synchronization venues IAW CCMD Procedures.

Certain tasks may require clearance up to the Top Secret/Sensitive Compartmented Information (TC/SCI) level, access to Special Access Programs (SAP), or access to Alternate Compensatory Control Measures (ACCM).

C.6.1.1.27. INSIDE PLANT (ISP)/ PROTECTIVE DISTRIBUTION SYSTEM (PDS) ENGINEERING AND INSTALLATION [*EXERCISED*]

The contractor shall provide engineering and installation services to support the build-out of identified facilities on-site at CJTF-HOA with requisite communications and IT infrastructure. Contractor presence may also be required to support inside plant activities at CJTF-HOA FOLs on a temporary basis.

C.6.1.1.27.1. PASSIVE INFRASTRUCTURE DESIGN AND INSTALLATION SERVICE

The Contractor shall install, remove, modify, and maintain passive infrastructure inside existing or newly constructed/remodeled buildings. Such passive infrastructure may include, but not be limited to, simple distribution system, protected distribution system (e.g. alarmed, etc.), raceway and/or stack connectivity between floors and communications closets, air-gap boxes and similar devices, patch panels and similar devices, and all other forms of connectivity (regardless of media type) not directly connected to a power source.

The Contractor shall install, remove, modify, and maintain communications and IT end user devices inside existing or newly constructed/remodeled buildings. Such communications and IT end user devices may include, but not be limited to alarmed carrier components, desktop computers, monitors, multi-system switching devices, desktop VTC, scanners, printers, telephones (analog and digital), secure telephone equipment (STE), and all other end user devices connected to a form of communications or IT network.

The Contractor shall perform network drop additions, moves, and removals. The Contractor shall acquire, install and integrate all components necessary to implement an Internal Cable Distribution and Protected Distribution System (PDS) to support NIPR and SIPR network access in accordance with the requirements set forth in this PWS. The Contractor shall supply all material and labor to install, integrate, test and make NIPR and SIPR passive infrastructure operational, minus the active infrastructure. The Contractor shall provide a site survey, on/off-site engineering, Bill of Materials (BOM) identification and procurement, site

preparation, installation, verification testing and quality control for all internal NIPR and SIPR passive infrastructure projects/service requests approved by the COR.

This work is expected to include projects ranging from temporary facilities (i.e. tents) to Containerized Work Unit(s) to hardened facilities and may include communication rooms and/or server rooms. The work may include anything from adding infrastructure to existing facilities to renovation of facilities to new construction. Projects will be classified into Type A or Type B based upon the recommendation of the Contractor and concurrence of the Government.

- Type A projects generally are smaller projects which could include tents, CWUs, or a few rooms within a hardened facility.
- Type B projects generally are larger in scale normally include new construction and major renovation of harden facilities but could also include multiple CWUs or tents.

C.6.1.1.27.2. PHYSICAL PLANT CONFIGURATION MANAGEMENT SERVICES

AFRICOM leverages a comprehensive Configuration Management System (CMS) that consolidates the IT physical plant and supporting passive infrastructure/connectivity data in one repository. The intent of the CMS is to provide for centralized management across various regions of the physical plant, thereby streamlining physical plant maintenance; reducing operational management costs and leveraging Critical Infrastructure Information to aid in identifying service faults and expedite troubleshooting. The CMS incorporates Inside Plant, Outside Plant, Data Center, WAN, Cable, and Circuit management in one place, providing AFRICOM with the oversight necessary to maintain critical operations. The CMS brings together data normally kept in disparate spreadsheet, CAD, and home-grown database files to create a more complete visual picture of an enterprise IT network environment.

The Contractor shall use the AFRICOM CMS to document, manage and track Critical Infrastructure Physical Plant Management data for the Inside Plant, Data Center, and Wide Area Network. The Contractor shall use the CMS to provide the following support:

- Physically trace end to end transmission paths throughout the local network
- Highlight physical circuit traces and actual routing in order to visualize redundancy and physical separation of mission-critical services
- Manage data center equipment rack elevations
- Manage data center Multi-Tiered Space/Floor plans
- Provide multi-dimensional data center power management

C.6.1.1.27.3 OUTSIDE PLANT SERVICES (OSP)

The Government desires limited Outside Plant services for the Forward Operating Locations (FOLs). The Contractor shall install, remove, modify, and maintain passive infrastructure outside (between) existing or newly constructed/remodeled buildings. Such passive infrastructure may include simple distribution systems, raceways, or other solutions. The work will only take place at the FOLs (vice Camp Lemonier) and will not include trenching. Performs cable splicing of fiber optic and/or twisted pair outside plant telecommunications cables.

The Government desires a solution that provides an OSP capability to the existing ISP team which will be used to work projects as assigned. This will be a level of effort requirement.

C.6.1.1.28. CASERMA DEL DIN NETWORK ~~ENGINEERING~~ ADMINISTRATION SUPPORT [*EXERCISED*]

The contractor shall provide an on-site presence at Caserma Del Din to perform network ~~engineering~~ administration services in support of the data center and AFRICOM Telecommunications Rooms. ~~This engineering effort is anticipated to be network centric; however, as projects expand it may branch into systems engineering, unified communications, and virtual infrastructure.~~ The systems under the Contractor's purview related to this support include local area networks and high-performance, high-availability server systems with emphasis on virtualized, hyper converged and application-centric infrastructures. This work requires knowledge of installing, operating, and repairing and decommissioning such systems.

The Contractor shall:

- ~~Interface with the local service provider(s) to ensure designs are coordinated and AFRICOM's enterprise architecture needs are met.~~
- ~~Provide network and system engineering designs, builds, and escalated support to services and products, to include supporting project management of systems and infrastructure.~~
- ~~Deliver services required for sustaining the transmission and/or communication path between geographically separated users/devices.~~
- ~~Install, configure, and transition IT systems to IT Operations Management.~~
- ~~Integrate and ensure interoperability of end user computing devices (e.g. desktops, laptops, and other portable devices) and peripherals with supported networks and communities of interest.~~
- ~~Provide image services on upgraded hardware.~~

- Operate and maintain and configure information systems hardware and software
- Install and maintain multi-platform networking computer environments, data networks, and telecommunications infrastructures
- Investigate, troubleshoot, and resolve end-user problems as directed by relevant USAFRICOM problem and/or incident management processes
- Coordinate with staff to inventory computer and communication systems under purview
- Monitor data center specific communication links and internal connectivity and report any discrepancies to the AFRICOM Network Control Center (ANCC) in accordance with standard operating procedures (SOPs)
- Diagnose issues, assess performance, and implement strategies to ensure systems availability
- Evaluate existing technology and provide recommendations for future modifications and/or replacement
- Respond to systems issues and manage the investigation, mitigation, and recovery of the issues applying diagnostic, corrective and recovery techniques to all facets of the integrated information systems
- Develop, maintain, and enforce site-specific standard operating procedures (SOPs) in accordance with USAFRICOM and DoD guidance
- Maintain and update configuration management database (CMDB) for any/all configuration items and systems under their purview

~~The Contractor's engineering processes may span other areas of this PWS.~~

~~Note: It is anticipated that this support will need to be supplemented in the future with additional resources. These resources could be in the form of Government Civilians, Active Duty, CITS personnel, or other contractors.~~

The following knowledge and skills are required:

- Network certification: Cisco Certified Network Associate (CCNA), or equivalent
- Security certification, IAT Level II

C.6.1.1.29. AFRICOM MOBILE COMMUNICATIONS SUPPORT [*EXERCISED*]

The Contractor shall provide AFRICOM with mobile communications support and maintain lines of cellular service from AFRICOM's cellular service provider.

The Contractor mobile communications support shall include:

- Provision new lines of service alongside the cellular service provider
- Maintain appropriate contract options, perform analysis of service options, and make recommendations to the Government on where efficiency or cost savings can be gained
- Maintain accountability of mobile devices through industry best practices for asset management systems or portals approved by the Government.

The Contractor shall provide Tier I support for all devices within the Mobility program at AFRICOM. The Contractor shall provision devices through DISA's Mobile Device Management (MDM) currently MobileIron, utilizing Defense Enterprise Provisioning Online, acting as DISA Purebred Trusted Agents, and other systems required to support Mobile Devices.

Reference PWS Section C.5.2.2.13. for general mobility support requirements.

C.6.1.1.30. AFRICOM ADVANCED NETWORK OPERATIONS AND ENGINEERING SUPPORT [*EXERCISED*]

The Contractor shall perform expert-level network and system communication integration activities for transition of enhancement and/or new capabilities to operations and sustainment. This includes transition services to ensure any changes to existing baselines capabilities are in accordance with AFRICOM engineering processes.

The Contractor shall:

- Engineer, integrate, operate, and maintain the National Security Agency (NSA) based Commercial Solutions for Classified (CSfC) program at USAFRICOM. (Reference PWS Section C.5.2.2.20.)
- Maintain the existing Data At Rest (DAR) Capabilities Package, along with any future Capability Packages that USAFRICOM requires. Maintenance of the Capability Package includes: performing the CP registration with NSA; development and submission of the annual re-registration; creation of applicable policies and training materials; and conducting end-user training. The Contractor shall provide security administration and auditing services within the construct of the guidance provided in the NSA Capability Packages.
- Fully architect, manage, and execute AFRICOM's Coalition enclaves (AMNET and future Mission Partner Environment and MNIS systems). Work includes the expansion of the AMNET architecture utilizing virtual data center (VDC) core services and tactical extensions.
- Integrate, implement, test, and perform verification and validation against test and deployment documentation for hardware and software at sites designated by the Government.

- Develop cybersecurity documentation in accordance with the DoD approved Risk Management Framework (RMF) processes.

Required certification:
Cisco Certified Internetwork Expert (CCIE)

C.6.1.1.31. AFRICOM ADVANCED COMMUNICATION CAPABILITIES ANALYSIS, PLANNING AND ASSESSMENT [*EXERCISED*]

This effort provides technical and lead C4 advanced engineering and operations support services to the Headquarters AFRICOM J6 (ACJ6) communication and network capabilities and operations including specialized solutions. The IT systems are for strategic current in-garrison and theater-wide employment as required to include: network engineering and operations, systems and virtualization, data storage, Information Assurance / Computer Network Defense (IA/CND), mobility solutions, Commercial Solutions for Classified (CSfC) solutions, Cyber Security and Defensive Cyber Operations (DCO), network infrastructure, enterprise desktop services (Unified Capabilities, Virtual Desktop, VTC, A/V), software and web-based tools and capabilities, architecture assessment, and performance improvement analyses.

The Contractor shall:

- Document and maintain program plans, technical plans, engineering requirements, design documentation and business processes to efficiently plan, coordinate and perform requirements and feasibility analysis and assessments of new or innovative IT network communication capabilities for AFRICOM.
- Review the existing UAFRICOM architecture and establish a baseline "current state" of the overall IT/communications architecture including network and transport topography, Cyber Defense / Information Assurance posture, and systems status.
- Develop systems architecture designs, as well as provide validation of integration processes, perform detailed systems analysis and design for development of operational/functional, systems, and technical architectures.
- Provide advanced communication program technical support, planning, analyses, assessments and evaluation to AFRICOM network and communication services project initiatives and activities.
- Provide detailed systems and design analysis documentation, topology diagrams, network drawings, system documentation, and capability plans will be maintained by the Contractor and the Contractor shall recommend and implement Information Technology (IT) Communications capabilities as directed by the ACJ6.
- Perform business process analysis; requirements definition and produce program documentation. Work includes the drafting of technical documentation including but not limited to: test plans and procedures, specifications, white papers, equipment and/or system training materials and technology description documents.

The Contractor shall assist in Cybersecurity assessments and reviews to ensure compliance with applicable regulations and guidance.

C.6.1.1.32. ~~CJTF-HOA~~ USAFRICOM FORWARD OPERATING LOCATION (FOL) SERVICES [*EXERCISED*]

The Contractor shall provide 24/7/365 on-site support services ~~presence~~ to Forward Operating Locations (FOLs) within the USAFRICOM AOR, on a permanent and/or temporary basis, as needed, which can change

from time to time, dependent on mission needs. ~~each site – Baledogle Military Airfield, Somalia; Manda Bay, Kenya; and Mogadishu Base Cluster, Somalia –~~At the time of executing an option for support, the Government will provide details of the FOL site and the required support services. At a minimum, the Contractor shall ~~to~~ provide services consisting of network services, end user device services, and logistics services.

Core duty hours at each site needs to be flexible to meet mission needs, generally the Contractor shall be required to provide services for six (6) 10-hour days each week. The hours may vary depending on military operations; however, the Government should provide at least 24-hour notice for deviations from normal schedules. Due to the critical nature of this support, the Contractor shall be on-standby when not on duty.

~~Services required at each site consist of:~~

- ~~Desktop Support Services as described in PWS Section C.5.2.1.3.1.~~
- ~~Print Services as described in PWS Section C.5.2.2.4.~~
- ~~VTC End User Support as described in the last bullet of PWS Section C.5.2.2.11.~~
- ~~IP Voice Services as described in PWS Section C.5.2.2.12.~~
- ~~Assist transport service provider with fault isolation~~
- ~~Provide Local Area Network Services as described in PWS Section C.5.2.2.15.2.~~
- ~~Provide limited Logistics Management services as described in PWS Section C.5.2.2.26. by providing purchasing and following CJTF HOA's configuration and asset management program along with managing the site's Life Cycle Management Program~~

C.6.1.1.32.1 BALEDOGLE MILITARY AIRFILED SUPPORT [*EXERCISED FOR CLDJ N6/DJIBOUTI*]

Baledogle Military Airfield (BMA), Somalia requires SIPR and NIPR services for its approximately 220 users. Each user will have a desktop consisting of a workstation/laptop and IP phones per network (SIPR and NIPR). In addition, there are approximately 30 multi-functions print devices per network, 4 SIPR desktop VTC devices, and 1 SIPR VTC suite.

Services required at this site consist of:

- Desktop Support Services as described in PWS Section C.5.2.1.3.1.
- Print Services as described in PWS Section C.5.2.2.4.
- VTC End User Support as described in the last bullet of PWS Section C.5.2.2.11.
- IP Voice Services as described in PWS Section C.5.2.2.12.
- Assist transport service provider with fault isolation
- Provide Local Area Network Services as described in PWS Section C.5.2.2.15.2.
- Provide limited Logistics Management services as described in PWS Section C.5.2.2.26. by providing purchasing and following USAFRICOM/CLDJ configuration and asset management program along with managing the site's Life Cycle Management Program

~~**[*EXERCISED*]**~~

~~Manda Bay (Camp Simba) requires SIPR and NIPR services for its approximately 25 users. Each user will have a desktop consisting of a workstation/laptop and IP phones per network (SIPR and NIPR). In addition, there are approximately 4 multi-functions print devices per network, 2 SIPR desktop VTC devices, and 1 SIPR VTC suite.~~

C.6.1.1.32.2 MOGADISHU BASE CLUSTER SUPPORT [*EXERCISED FOR CLDJ N6/DJIBOUTI*]

Mogadishu Base Cluster, specifically the Military Advisory Group – Somalia (MAG-S) within the Military Coordination Cell (MCC), requires SIPR and NIPR services for its approximately 25 users. Each user will have desktop consisting of a workstation/laptop and IP phones per network (SIPR and NIPR). In addition, there are approximately 4 multi-functions print devices per network, 2 SIPR desktop VTC devices, and 1 SIPR VTC suite.

Services required at this site consist of:

- Desktop Support Services as described in PWS Section C.5.2.1.3.1.
- Print Services as described in PWS Section C.5.2.2.4.
- VTC End User Support as described in the last bullet of PWS Section C.5.2.2.11.
- IP Voice Services as described in PWS Section C.5.2.2.12.
- Assist transport service provider with fault isolation
- Provide Local Area Network Services as described in PWS Section C.5.2.2.15.2.
- Provide limited Logistics Management services as described in PWS Section C.5.2.2.26. by providing purchasing and following USAFRICOM/CLDJ configuration and asset management program along with managing the site's Life Cycle Management Program

C.6.1.1.32.3 AFAF FORWARD OPERATING LOCATION (FOL) SERVICES [*EXERCISED FOR AFAF*]

US Air Forces Africa (AFAFRICA or "AFAF") A6 intends to significantly reduce its forward-deployed tactical communications equipment and personnel at several sites on the African continent. In accordance with the USAFRICOM J6 strategy to leverage joint NIPR and SIPR transport and AFRICOM Information Environment (ACIE) network services where possible across the continent, AFAF intends to extend AFRICOM network services to their East Africa (EA) sites. ~~AFAFRICA (~~AFAF~~)~~ requires on-site support services to East Africa (EA) Forward Operating Locations (FOLs) – specifically Manda Bay, Kenya and Chabelley Airfield, Djibouti. The contractor shall provide services consisting of network services, end user device services, and logistics services in support of these sites.

To support EA forward sites, AFAF requires on-site, dedicated, Logistics Management services as described in PWS Section C.5.2.2.26. and subsections. AFAF assets for EA sites are currently managed out of Camp Lemonnier, Djibouti (CLDJ) prior to forward deployment. Support services for Logistics Management are predominately performed at CLDJ; however, the contractor may be required to provide on-site presence at EA sites on a routine or temporary basis to support asset management activities.

C.6.1.1.32.3.1 MANDA BAY SUPPORT [*EXERCISED*]

Manda Bay (Camp Simba), Kenya requires on-site SIPR and NIPR services for its approximately ~~25~~ 600 users. Each user will have a desktop consisting of a workstation/laptop and IP phones per network (SIPR and NIPR). In addition, there are approximately ~~4~~ 20 multi-functions print devices per network, ~~2~~ 8 SIPR desktop VTC devices, and 1 SIPR VTC suite.

Services required at this site consist of:

- Desktop Support Services as described in PWS Section C.5.2.1.3.1.
- Print Services as described in PWS Section C.5.2.2.4.
- VTC End User Support as described in the last bullet of PWS Section C.5.2.2.11.
- IP Voice Services as described in PWS Section C.5.2.2.12.
- Assist transport service provider with fault isolation
- Provide Local Area Network Services as described in PWS Section C.5.2.2.15.2.
- Provide limited Logistics Management services as described in PWS Section C.5.2.2.26. by providing purchasing and following USAFRICOM/AFAF configuration and asset management program along with managing the site's Life Cycle Management Program. The preponderance of Logistics Management services can be performed remotely from Camp Lemonnier, Djibouti with occasional travel, as needed, to Manda Bay in support of service requirements.
- Service Desk Support described in PWS Section C.5.2.1.1.
- Account Management as described in PWS Section C.5.2.1.2. and subsections

Note: Support services at Manda Bay are currently augmented by military personnel for Desktop Support Services, Print Services, and VTC End User Support. It is anticipated that this support may need to be supplemented in the future with additional contractor resources as usage increases or if there is a reduction in supplemental support being provided by military forces.

C.6.1.1.32.3.2 CHABELLEY AIRFIELD SUPPORT [*EXERCISED*]

~~Chabelley Airfield, Djibouti (CADJ) requires remote desktop operations and maintenance support with limited on-site SIPR and NIPR services for its approximately 25 users on an as needed basis.~~ AFAF intends to significantly reduce its forward-deployed tactical communications equipment and personnel at Chabelley Airfield, Djibouti (CADJ) by fully extending AFRICOM Information Environment (ACIE) network services at the base. Currently, AFAF is reliant on a limited USAFRICOM Local Area Network providing AFRICOM NIPR and SIPR services from Camp Lemonnier, Djibouti (CLDJ) to a small footprint of approximately 25 users. CADJ requires AFRICOM network migration with on-going operations and maintenance support for an initial 250 NIPR and 75 SIPR users with infrastructure capacity provisioned to support 300 NIPR and 100 SIPR users. This network extension has been designed around a USAFRICOM enterprise network standard, will be an extension from CLDJ, and the architecture and infrastructure will be implemented to allow remote management from CLD. The installation and maintenance of network fiber and cabling is currently being supported by military personnel; however, inside plant and limited outside plant support may be required in the future.

~~Limited s~~Services~~, on a non-recurring basis,~~ required at this site are consistent with O&M services required at Camp Lemonnier and consist of:

- IT Service Management as described in PWS Section C.5.1.6.
- End User Support as described in PWS Section C.5.2.1.1. and associated subsections. (*Note: Support functions such as Service Desk may be accomplished remotely at CLDJ.*)
- Desktop Support Services as described in PWS Section C.5.2.1.3.1.
- Enabling Services as described in PWS Section C.5.2.2.1. and associated subsections. *(Note: Limited to client services only.)*
- Image Services as described in PWS Section C.5.2.2.3.
- Print Services as described in PWS Section C.5.2.2.4.
- VTC End User Support as described in the last bullet of PWS Section C.5.2.2.11.
- IP Voice Services as described in PWS Section C.5.2.2.12.
- Provide Local Area Network Services as described in PWS Section C.5.2.2.15.2.

- Provide limited Logistics Management services as described in PWS Section C.5.2.2.26. by providing purchasing and following USAFRICOM/AFAF configuration and asset management program along with managing the site's Life Cycle Management Program. (*Note: The preponderance of Logistics Management services can be performed remotely from Camp Lemonnier, Djibouti with occasional travel, as needed, to Chabelley in support of service requirements*).
- Assist transport service provider with fault isolation

Network systems availability and support must be sufficient to support 24/7 flying operations at CADJ and service levels must match the Critical Success Factors defined for "Djibouti". On Call Support as described in PWS Section C.5.1.4. for CADJ will be the same as Djibouti/CLDJ for responding telephonically to an outage within 30-minutes of initial notification and will be doubled from the Djibouti/CLDJ response time for responding on-site with response time for CADJ being within 2 hours of initial notification.

C.6.1.1.33 ENHANCED ISKM REQUIREMENTS [*EXERCISED FOR EUCOM*]

C.6.1.1.33.1 CUSTOM ISKM DEVELOPMENT

The contractor shall provide custom ISKM development support for the planning, design, and development of software applications with the following duties;

- Quickly learn and implement new ISKM and web technologies
- Function effectively within an Agile development environment utilizing Scrum processes for software lifecycle management.
- Collaborates with a Product Owner and testing teams to develop, test, and refine the applications to meet stakeholder requirements, integrating both .NET Controls and Web Service implementations as part of the overall Knowledge Management architecture.

STAFFING REQUIREMENTS

- Full stack development with extensive .NET experience
- Proficient with development of SQL queries in a MS SQL Server environment
- Microsoft Certified Solution Developer (MCSD)

C.6.1.1.33.2 ISKM DEVELOPMENT LAB MANAGEMENT

The contractor shall provide the day to day maintenance of a test and development lab for Software Systems Integration.

- Provide troubleshooting and problem resolution for classified and unclassified Microsoft Server Operating System technologies including Windows Server 2008 R2, Windows Server 2012 R2, and Windows Server 2016 for Knowledge Management development team.
- Review, research, and apply system and application patches, hotfixes, service packs, and security configuration for CYBERCOM and DISA STIG compliance.
- Manage enterprise Active Directory forests, AD-Integrated DNS, Group Policy Objects, External DNS, DHCP, and Distributed File Services. Ensures infrastructure standards are in compliance with Command policies, audit requirements and ensures potential security risk are mitigated and documented.
- Manage cloud resources in the selected DoD-approved cloud environment as required.
- Propose and implement test and development lab upgrades that would improve the capability and functionality of the lab.

STAFFING REQUIREMENTS

- Experience with Adobe Creative Suite
- Experience developing user interfaces for SharePoint 2016/2019
- Experience with industry standard wireframing.

C.6.1.1.33.3 BATTLE RHYTHM MANAGEMENT

The contractor shall provide support related to development, coordination, assessment, training and management of the EUCOM Battle Rhythm, in direct support to the Chief of Staff. This function is integral to the Knowledge Management (KM) Program, which serves a diverse customer base with far-reaching implications, in support of steady state and crisis action operations. The Command's leadership identify KM management of the Command Battle Rhythm as pivotal to staff integration and the execution of efficient decision making processes.

STAFFING REQUIREMENTS

- Extensive experience with full battle rhythm lifecycle at a joint headquarters environment or equivalent
- Experience presenting at the General Officer / Flag Officer (GO/FO) Level
- Experience in joint planning/ops at a military HQ level
- Experience with Business Process Analysis and Engineering
- Strong proficiency in Microsoft SharePoint, Office Suite, Visio and PowerPoint.

Familiarity with business process engineering methodologies & frameworks (eg. Lean Six Sigma).

C.6.1.1.33.4 ISKM DESIGN

The contractor shall collaborate with Product Owners and technical teams to extract project requirements and illustrate design concepts using storyboards, process flows, and sitemaps.

- Provide expert knowledge of typography and typographic principles, branding and design experience for responsive web, color theory, and have an eye for modern design.
- Provide basic design utilizing tools in the Adobe Creative Suite
- Provide technical web development knowledge to understand technology limitations and capabilities for both SharePoint tools and custom developed solutions in .NET/Angular/Bootstrap.
- Design elegant, simple, human-centric flows and experiences as the Command define new initiatives and iterate on existing features.

STAFFING REQUIREMENTS

- MCSA Windows Server 2016
- Experience administering VMWare, Azure
- Extensive windows administration background, including Active directory and group policy management
- Experience administering windows servers including Exchange, and DCs

OTHER REQUIREMENTS

All must possess IAT Level II certification(s) IAW DoD 8570.1

All must possess TS/SCI security clearances

C.6.1.1.34. USARAF COMMUNICATIONS PLANNING AND NETWORK OPERATIONS [*EXERCISED*]

USARAF requires communications planning and network operations support. The Contractor shall, consistent with technical direction provided by the Government, serve as the communications integrator responsible for the planning, coordination, employment, operation, and management of tactical and commercial communication systems and IT networks in support of the USARAF AOR. The Contractor shall provide technical and tactical advice to command and staff on IT matters and signal architecture design at the ASCC level. The Contractor shall be responsible for the base lining, validation, and deployment of communication packages. The Contractor shall be responsible for planning both near-term and long-term operational communications plans support to seven (7) named operations, four (4) contingency plans, and eleven (11) contingency locations on the continent of Africa in support of the Combatant Commander. The Contractor shall refine and improve Operational Plans (OPLANS), Operations Order (OPORD), communication annexes, and appendixes. The Contractor shall develop communication branch plans and assess both near-term and long-term communications plans throughout the organization. The Contractor shall establish coordination and liaison relationships with DoD organizations and host nations, as required.

The Contractor shall participate and support Multi-National planning events, Theater Security Cooperation (TSC) events, Mission Assurance Assessments (MAA), spectrum management, mobile communications capability, and Network Operations (NETOPS) as follows:

- **Multi-National Planning Events**. The Contractor shall participate and support initial, mid and final planning events. Additionally, as required, the Contractor shall participate in command exercise planning working groups. The Contractor shall provide tactical and technical advice during planning events and collect unit requirements for exercise planning. The Contractor shall coordinate with host nation communication planners, sources local communications equipment, conducts market research, develops communications minutes and assists during execution phase of exercises. The Contractor shall develop initial communications architecture consistent with technical direction provided by the Government.
- **Theater Security Cooperation (TSC) Events.** The Contractor shall ensure G6 communications functions are developed, integrated, and executed for all pertinent USARAF TSC and US Military to African partner Military (M2M) events both locally and on the African continent. The Contractor shall work closely with USARAF's Security Cooperation Directorate (SCD) to ensure that G6 communications efforts are integrated into the USARAF mission set for security cooperation events and the M2M engagements in support of USARAF's Supporting Campaign Plan Lines of Effort and USAFRICOM's Theater Campaign Plan goals.
- **Mission Assurance Assessments (MAA).** MAA is the DoD program of record for evaluating the force protection conditions at installations worldwide and is USARAF's means of understanding and mitigating on-site risks to personnel and/or property. USARAF is required to complete an annual MAA on all sites under USARAF's Base of Operations Support – Integrator (BOS-I) control. Based on the risks identified by the MAA team, USARAF develops plans and policies for the site and submits equipment and resource requests to the USARAF requirements board for funding. The Contractor shall focus on the G6 equities pertaining to communications infrastructure and architecture during the MAA.
- **Spectrum Management**. The Contractor shall provide guidance to the staff and commanders on all spectrum related matters, coordination, deconfliction, and issue of spectrum resources; directly coordinates with supporting elements of USARAF to ensure spectrum resources are properly allocated in a timely manner.

- **Mobile Communications Capability.** The Contractor shall coordinate, track, and resource mobile communications requirements on the continent of Africa. The Contractor shall work with elements supporting USARAF on the continent by validating Primary, Alternate, Contingency, and Emergency (PACE) plans and directly coordinate with USARAF's Telecommunications Officer (TCO) to ensure resources are available to meet mission requirements.
- **NETOPS Support System (NSS).** The Contractor shall be required to utilize the ITSM Trouble Ticket system to record NETOPS outages and HAZCON events and assign to the appropriate supporting authority. This includes both NIPR, SIPR, Mission Partner Environment (MPE) networks and extends to all workload associated with audio, video, video teleconferencing (VTC), and data communications capabilities and services supporting USARAF on the continent of Africa. In all instances, workload will be captured/documented and tracked via ITSM ticket reference regardless of whether NIPR, SIPR, MPE, VTC or other support functions.

The Contractor will be required to deploy to the continent of Africa to support the above mission sets four (4) to eight (8) times a year for periods ranging from three (3) to thirty (30) days. In case of surge/emergency requirements, the contractor may be required to exceed thirty (30) days.

Normal duty hours for dedicated support requirements are 0800 to 1700 hours local time five (5) days a week, Monday through Friday, excluding Federal Holidays. The Contractor may have employees work flexible hours, if necessary, outside of the 0800 to 1700 hours timeframe, as long as there is no mission impact during the core duty timeframe and coordination with the COR(s)/TPOC(s) has occurred. The Contractor shall at a minimum attend weekly G6 Operations Synchronization meetings, G6 Directorate Huddles, weekly status updates, and other meetings as directed.

The Contractor shall respond to emergency calls within two (2) hours. USARAF may request surge manning for emergency or contingency/exercise requirements as directed in writing by designated Government representative. The Contractor shall provide support during surge operations with Contractor personnel available for 24x7 operations upon 48-hours' notice by the COR(s)/TPOC(s). A determination for a Special Tasking, dependent upon Surge/Emergency Requirements of USARAF can be considered for additional support requirements that meet these criteria.

It is expected that Contractor personnel must:

- Obtain a valid U.S. Official Passport.

The following knowledge and skills are preferred:

- Minimum four years of experience with U.S. Army tactical communications assemblages.
- Minimum three years of experience serving in a managerial position and/or project manager.
- Military service as a senior leader.

The Government estimates a minimum Level of Effort of four (4) full time equivalents (FTE) to perform the functions identified above.

C.6.1.1.35. ELECTROMAGNETIC SPECTRUM FREQUENCY MANAGEMENT SUPPORT [*EXERCISED FOR AFRICOM*]

The Contractor shall provide technical expertise and guidance on the use and management of the electromagnetic spectrum.

The Contractor shall:

- Establish and update command policy for managing, requesting, and coordinating the use of the electromagnetic spectrum (EMS), Joint Restricted Frequency List (JRFL) process, and Communications Electronics Operating Instructions (CEOI) process.
- Gather spectrum use requirements to conduct operation and contingencies, as required.
- Obtain, via Spectrum XXI or other authorized means, spectrum resources to conduct operations and contingencies, as required.
- Identify, report, and resolve electromagnetic interference (EMI).
- Provide liaison between Major Subordinate Commands (MSC), higher headquarters and/or other senior spectrum management agencies including coordination among Ground Task Force operations within the electromagnetic environment.
- Support development and procurement of spectrum operations tools and policy.
- Provide recommendations to the Government for manning, training and equipping all spectrum operations.
- Maintain and promulgate a common frequency database for planning, coordinating, and controlling spectrum use.
- Identify, evaluate, and provide resolution guidance to potential spectrum use conflicts.
- Develop, update, and distribute a signal operating instruction (SOI)/CEOI and shall support the controlling authority.
- Develop, update, and distribute the JRFL.
- Ensure Information Operations (IO) plans are supportable within the spectrum management architecture.

It is expected that Contractor personnel will require:

- Completion of formal Spectrum XXI training.

The following knowledge and skills are preferred:

- Demonstrated experience with US military frequency management. Must understand all aspects of Radio Frequency (RF) systems including UHF, VHF, HF, and EHF.
- Demonstrated experience developing spectrum management plans including CEOI and JRFL.

C.6.1.1.36. EUCOM LOGISTICS FUNCTIONAL AREA SYSTEM (LOGFAS) INTEGRATION

The U.S. European Command (EUCOM) logistics directorate (ECJ4) uses a host of different logistics applications to execute and manage logistics operations. These systems are individually managed and do not support data sharing. This problem is further complicated since each of the CCMD's components and coalition partners uses their own systems. ECJ4 has a requirement for contractor support regarding strategic resourcing decisions, joint and combined planning, and execution of current operations and exercises by integrating disparate information systems and data repositories.

The contractor shall:

Facilitate the planning and integration of data sets between the various logistic systems with primary work on the eucom.mil domain.

- Support logistic information management systems to inform strategic resourcing decisions, joint planning and the execution of operations and exercises.
- Develop data sharing strategies - plan data structures and data sharing between disparate logistical systems.

- Provide project management oversight in the integration of Information Management Systems between each of the components and coalition partners.
- Establish a data flow hierarchy with subordinate commands and coalition partners.
- Build Oracle based queries to extract data from command and coalition partner information systems to extract information and display in dashboards to leadership.
- Handle general updates and configuration changes/requests for J4 managed IT systems.
- Advise J4 staff on technical implementations and integration of J4 Information Management systems with components and coalition partners.
- Identify system deficiencies and recommend solutions.
- Provide maintenance and continuous improvement of the processes, standards, policies, working methods, and tools.
- Develop a functional knowledge of systems such as US DoD Joint Operational Planning and Execution System (JOPES), NATO Logistics Functional Area Services (LOGFAS), USEUCOM Mission Partner Environment (MPE), Battlefield Information Collection and Exploitation System (BICES), Standard Base Supply System (SBSS) and Global Combat Support System- Army (GCSS-A), Marine Corps (GCSS-MC) and Joint (GCSS-J), Single Mobility System (SMS), among other systems.

Personnel Requirements:

- Minimum Secret clearance.
- DoD 8570 IAT II compliant.
- Familiarity with US DoD logistics processes and systems.
- Experience working at the CCMD level providing IT / Communications support.

Place of Performance:
HQ USEUCOM, Logistics Directorate (ECJ4), Patch Barracks, Stuttgart Germany.

C.6.1.1.37. DATABASE MANAGEMENT AND ADMINISTRATION [*EXERCISED FOR AFRICOM*]

The Contractor shall:

- Provide SQL infrastructure engineering to include database architecture maintenance, database upgrades, server configurations, and application configurations.
- Install, configure, and manage multiple SQL server environments with high availability and disaster recovery, to include monitoring, analysis, reporting, and data warehouse services and solutions
- Architect and design the configuration and operation of SQL platforms on all AFRICOM environments.
- Ensure proper integration of SQL with applications to include but not limited to SharePoint, TMT, Active Directory.
- Provide best practice recommendations related to SQL maintenance procedures, SQL application integration procedures, and design of the overall SQL infrastructure on all AFRICOM domains.
- Operate and maintain the front and back end SharePoint infrastructure and perform incident management.
- Perform front/back end infrastructure engineering, capability engineering and application integration (primarily MS applications), front/back end infrastructure engineering, and incident management.
- Perform server O&M for custom collaboration tools (SLCS, Enterprise Calendar, AFRIT, TMT)

Note: Contractor must possess an understanding of Windows clustering technology to support various SQL clusters and SQL Always On Availability Groups.

Required certification:

- MCSE: Data Management and Analytics, or newer equivalency

C.6.1.1.38. IDENTITY AND ACCESS MANAGEMENT [*EXERCISED FOR AFRICOM*]

The Contractor shall:

- Develop the architecture, design and standards of Identity Management infrastructures including Active Directory, SAML, ADFS, FIM, Azure, Meta-Directories, Enterprise Authentication, Single Sign-on and Provisioning systems.
- Establish standards for directory and application integration as well as implementing solutions to successfully integrate new technology with existing and new architectures.
- Architect and design the configuration and operation of identity management solutions to support AFRICOM initiatives and interoperability between the command and its partners.
- Perform Microsoft Identify Management (MIM) system capacity analysis and planning, and optimize system operation/resource utilization.
- Provide guidance to operations personnel for operation and troubleshooting of identity management solutions.

C.6.1.1.39. SOFTWARE MAINTENANCE [*EXERCISED FOR AFRICOM*]

The contractor shall provide technical services in support of software development, configuration, modifications and maintenance efforts associated with, but are not limited to, ASP.NET applications and SharePoint applications using JavaScript/ JQuery, React, and Angular. The Contractor shall have the expertise to integrate software with all variants of Microsoft SharePoint, Microsoft 365, and Microsoft Exchange.

The existing custom applications that will be managed and maintained include (AFRIT, Command Calendar, SLCS, TMT):

- A budget management system
- A specialized calendar used to coordinate activities across the organization
- A specialized calendar that tracks events and executive travel.
- A portal that used to collaborate on current operations related activities.

Changes/corrective action may be required for functional capabilities or implementation of mitigations associated with cyber-security /vulnerabilities, or as required by applicable Security Technical Implementation Guides (STIGs). The contractor shall maintain awareness of STIGs that affect the source code, source code language or operating systems that applications operate under. The contractor shall coordinate with appropriate systems administrators to ensure database and system backups/account management.

The contractor shall work with the Government to gather and document corrective action or new requirements; rewrite/upgrade existing applications; integrate applications into the production environment; migrate current data to the applications; develop, test, launch, manage and operate the system.

The contractor must have demonstrated experience in .NET applications, Angular, Microsoft technologies such as SharePoint, Office 365, systems, and technical functions such as the design, maintenance, administration, training, integration, testing, and/or software configuration of technology.

Required certifications:

- CompTIA Security + (or newer)
- IAT Level II (or greater)
- ITIL v3 or v4 – Foundation
- MCSD certification, or newer equivalency

C.6.1.1.40. SCRIPTING/APPLICATION INTEGRATION [*EXERCISED FOR AFRICOM*]

This effort involves technical services in software maintenance, modification and customization associated with integrating external resources and data sources to an IT service management platform. The Contractor shall integrate software via Application Program Interfaces (APIs) using one or more of the following technologies: scripting, JavaScript, REST (representational state transfer), SOAP (simple object access protocol), JSON web services, ODBC (Open Database Connectivity). The contractor must have demonstrated developmental experience in a multitude of the identified technologies.

The contractor shall work with the Government to gather and document corrective action or new requirements; rewrite/upgrade existing applications; integrate applications into the production environment; and migrate current data to the applications; develop, test, launch, manage and operate the system.

Required certifications:

- CompTIA Security + (or newer)
- IAT Level II (or greater)

Preferred qualifications:

- Experience with ServiceNow APIs and Integration Tools

C.6.1.1.41. COALITION AND BILATERAL NETWORK SECURITY CONTROL ASSESSMENTS (SCA) [*EXERCISED FOR AFRICOM*]

The contractor shall be responsible to certify Mission Partner's internal systems and infrastructure. The contract shall conduct security risk assessments for the authorizing official to authorize the existence and operation of the BICES bilateral networks. The contractor shall conduct validations of Information Assurance (IA), security posture, determine risk, and develop certification recommendations in support of accreditation for the Government.

This requirement encompasses the full scope of requirements as described in PWS Section C.5.2.2.22.5. RISK MANAGEMENT FRAMEWORK (RMF) and C.5.2.2.22.6. SECURITY CONTROL ASSESSMENTS (SCA). Reference PWS Section C.2.5.4. COALITION AND MULTI-DOMAIN (TO INCLUDE BI-LATERAL) NETWORKS for additional information regarding coalition network systems.

C.6.1.1.42. CURRENT OPERATIONS INTEGRATION CENTER (COIC) SUPPORT [*EXERCISED FOR SETAF-AF*]

The contractor shall provide support to the SETAF-AF Current Operations Integration Center (COIC), G6 Directorate in accordance with SETAF-AF COIC Procedures. The contractor shall serve as a focal point to maintain headquarters (HQ)-DoD information networks (DoDIN), situational awareness in support of

command and control (C2), accomplish command-wide communications infrastructure management, manage HQ and theater authorized service interruptions (ASI) programs, coordinate response to emergent cyber events, and mitigate operational impact resulting from significant theater and enterprise communication and service outages. The contractor is responsible for integrating all aspects of SETAF-AF G6 operations with the G33, to include, coordinating theater C2 event response with command headquarters, components, and global operations partners. To support the COIC, the contractor shall:

- Work closely with local, theater and global Joint Force Headquarters (JFHQ)-Department of Defense Information Network (DoDIN) agencies and support activities to facilitate theater operations situational awareness, issue mitigation, and a coordinated network defense posture.
- Identify problems, determine accuracy and relevance of a broad range of technical information, use sound judgment to generate, evaluate, and execute alternative courses of action for immediate mitigation of operational impact, and produce timely, effective, decision-quality technical recommendations to support senior leadership.
- Analyze, track, and coordinate authorized service interruptions (ASI) for the theater, to include all events impacting command, component, operating, and tactical locations.
- Provide communication systems analysis and cross-organization coordination expertise support continuous communications service to all C2, enduring, tactical, and mobile locations in the CCMD area of operations.
- Provide technical oversight of information security services and customer support initiatives.
- Provide guidance to the staff and commanders on all spectrum related matters and coordination and issue of spectrum resources.
- Assist with mobile device and Iridium support for SETAF-AF Request for Forces (RFF) and Regionally Aligned Force (RAF) personnel deployed to the continent.
- Represent SETAF-AF G6 concerning communications, IT policy, and problem resolution.
- Prepare and execute oral and written notifications, reports, and presentations on significant Command, Control, Communications, and Computers (C4) issues, status changes, and operational impacts for presentation to Flag and General-level officers and the command-wide operational and operations communities of interest.
- Attend weekly G6 Operations Synchronization meetings, G6 Huddles, weekly status updates, and other meetings as directed.

The Contractor shall oversee and manage all IT Service events and work orders that impact the SETAF-AF missions both on the continent and on the COIC floor, regardless of the type or service provider. Examples of these duties include:

- Initial troubleshooting for any IT system/device within the COIC.
- Reporting system outages to the appropriate service provider and following up with status inquiries until service is restored.
- Reporting and coordinating necessary actions with equipment vendors for warranty, service visits, and/or repair work.
- Providing weekly briefings to leadership on the status of all incidents and actions being tracked.

The contractor shall provide support for Joint Task Force (JTF) Operations as well as contingency operations/named operations on the continent.
Examples of tasks include:

- Monitoring of operational system and network status.
- Initial triage and troubleshooting of events and incidents.
- Coordination for escalated troubleshooting or support of events or incidents.

- ASI management.
- Tracking of cyber security incidents.

Support under this requirement requires knowledge and expertise in:

- **Information Technology (IT) Principles.** Expert level knowledge of, and skill in applying, advanced IT principles, concepts, methods, standards, and practices sufficient to accomplish assignments such as provide expert technical advice, guidance, and recommendations to management and other technical specialists on critical IT issues; apply new developments to previously unsolvable problems; and make decisions or recommendations that significantly influence important agency IT policies or programs.
- **Systems Administration (SA).** The contractor shall perform work detailed through IT Service Management (ITSM) requested by end-users via the Help Desk. This work shall include Systems Administration (SA) and Operation on the multi-user, multi-computer networks assigned (NIPRNet and SIPRNet), which provides Messaging Services (Email/Defense Message System (DMS)) and is a Gateway to the NIPRNet and SIPRNet for all end-users and computer systems located at the SETAF-AF footprint (to include TDY and deployed forces The Contractor will utilize Government provided tools to achieve compliance integration on the network, and make these tools available for other Information Management Officers (IMOs) on SETAF-AF/AFRICOM systems to use in the performance of their duties.
- **Network Administration.** The Contractor shall be familiar with basic networking concepts and will be responsible for providing first line fault monitoring on the customers networks making best use of available network management tools; Identify, isolate and classify network faults identified either manually or via available network management tools; Receive, confirm, and classify network reported faults identified by customers, event management systems, or performance management tools. They will provide assistance via remote access, phone, or in person.
- **NETOPS Support System (NSS).** The contractor shall be required to utilize the ITSM Trouble Ticket system to record NETOPS outages and HAZCON events and assign to the appropriate supporting authority. This includes both NIPR and SIPR and extends to all workload associated with audio, video, video teleconferencing (VTC), and data communications capabilities and services supporting SETAF-AF and on the continent of Africa. In all instances, workload will be captured/documented and tracked via ITSM ticket reference regardless of whether NIPR, SIPR, VTC or other support function.

C.6.1.1.42.1. OTHER CONSIDERATIONS

This requirement is part of the command Emergency Relocation Group (ERG) for continuity of operations (COOP) and is considered mission essential. Individuals performing mission essential functions must report for work in all threats and emergency situations (e.g., severe weather conditions, power failures, technological failures, terrorism events, and other natural and manmade disasters) in which significant numbers of employees are prevented from reporting for work or which require agencies to close all or part of their activities. ERG personnel may perform mission essential functions at an alternate location not later than 12 hours after COOP activation and to sustain operations 24/7 for a minimum of 30 days or until normal operations are resumed. The alternate location may potentially be an austere environment.

During an emergency situation, vacating a mission essential position would seriously impair the capability of the organization to function effectively. In the event of an emergency situation, the contractor must continue to perform the mission essential functions until relieved by proper authority (COR or TPOC).

The contractor will be required to take part in readiness exercises and must maintain readiness, with or without warning, to move to and work from an alternate location within the United States Army Europe and Africa (USAREUR-AF) Theater of Operations.

C.6.1.1.42.1.1. SECURITY REQUIREMENTS

Contractor personnel must hold a TOP SECRET security clearance with a Single Scope Background Investigation that grants them IT Level 2. The contractor shall provide personnel who are able to achieve and maintain the adjudicative standards set forth in the Intelligence Community Directive (lCD) Number 704 "Personnel Security Standards And Procedures Governing Eligibility For Access To Sensitive Compartmented Information and other Controlled Access Program Information."

Reference Section H.3.2. SECURITY PLAN

C.6.1.1.42.1.2. PERSONNEL QUALIFICATIONS.

The contractor must be compliant with DoD 8570. Required certifications include:

- IAT II
- Job-specific computing environment (CE) certification

Reference Section H.5. PERSONNEL QUALIFICATIONS

C.6.1.1.42.2 PLACE OF PERFORMANCE, DUTY HOURS, and RESPONSE TIMES

C.6.1.1.42.2.1 PLACE OF PERFORMANCE

Support services will be performed in the Headquarters (HQ) Southern European Task Force-Africa (SETAF-AF) Current Operations Integration Center (COIC), G6 Directorate, Vicenza, Italy. Upon direction, the position may be required to deploy on a temporary duty (TDY) basis to support JTF Operations, as well as contingency operations/named operations on the continent.

C.6.1.1.42.2.2 CORE/DUTY HOURS

Normal core/duty hours for the COIC are Monday through Friday from 0800 to 1700; however, the contractor will function as the singular G6 representative to the command while outside of regular business hours.

The contractor will, on order (O/O), provide up to 24/7 support to the COIC with the possibility for rotational shift work on the COIC floor in the event of contingency operations/named operations supporting missions on the continent will be considered. Potential rotational shifts may include:

- 24/7 rotational shifts: O/O continuous rotational shift work in a 24 hours-per-day, 7 days-per-week COIC watch.
- 16/7 rotational shifts with on-call coverage: O/O rotational shift work in a 16 hours-per-day, 7 days-per-week Joint C4S Fusion Cell (JCFS) watch. The remaining 8 hours must be covered by on-call support.

Rotational shifts may require the contractor to work overtime or provide augmented surge support.

C.6.1.1.42.2.3. RESPONSE TIMES

Emergency Calls. The Contractor shall respond to emergency calls within two (2) hours.

Overtime/Surge/Emergency Requirements. SETAF-AF may request, or the contractor may propose, overtime or surge manning for emergency or contingency/exercise requirements. The contractor shall provide support during emergency or contingency operations with personnel available up to 24/7 operations upon 48-hoursnotice by the Government.

C.6.1.1.43. EUCOM OFFICE OF DEFENSE COOPERATION (ODCs) SERVICES [*EXERCISED FOR EUCOM TSCMIS*]

The Contractor shall provide enhanced administration and support to include workgroup administration and Telephone Control Operations for 40 ODC sites in the USEUCOM Area of Responsibility (AOR).

- Serve as a Tier 1 point of contact for users regarding hardware, software and network-related (NIPRNet / SIPRNet) issues and/or requests.
- Manage and track new user and non-person Entity (formally known as Distribution or Organizational mailboxes) account requests / modification / deletions for network and Security Assistance (SA) system and ODC budget management system applications access within the non-binding target of two business days of receipt.
- Manage public drive folders and associated permissions assigned to their divisions.
- Submit network configuration changes (upgrades, fiber drops, workstation moves, etc.)
- Perform user system training and provide any needed assistance.
- Ensure ODC network and application access requirements are met and new hardware purchases comply with the EUCOM or (Department of state (DOS) C4I network architecture.
- Submit new requirements (PC, laptops, printers, etc.) via RMS, track requests, and coordinate pickups through the directorate Property Book Officer (PBO).
- Forecast Lifecycle Replacement (LCR) requirements for current plus two fiscal years for budget inputs. Submit LCR requirements to the EUCOM J6 Resource Management Board (RMB) and complete/update LCR requirement tickets in Service Manager; coordinate pick up through directorate ODC PBO.
- Coordinate the disposal of unserviceable/DRMO equipment; clear all equipment for disposition through proper agencies (52nd SIGNAL, ECJ6, etc.) and ODC PBO.
- Provide on-site touch maintenance and repair that could not be done remotely on an as-needed basis.
- Manage current and create new user guides as necessary to train users in IT access and operations procedures. Guides will be maintained on Directorate SharePoint or Partner's Portal Knowledge Management (KM) pages
- Assess network bandwidth to ensure network connectivity permits all applications to be used without interruption. Coordinate with local IT personnel (Department of State or commercial network service provider) to identify systemic issues between local provider and EUCOM network. Coordinate with Defense Security Cooperation Agency (DSCA) to ensure networks support application bandwidth requirements.
- Work to develop an Information Assurance (IA) compliant laptop image that can be remotely loaded on commercially procured government computers that permits 50 Mbps wireless upload/download speeds or better.
- Submit waiver requests for ODC personnel (USEUCOM and non-USEUCOM Members) requiring a Commercial Mobile Device (CMD) or Secure Mobile Device (SMD), and are not included as an approved user by ECI 8102.01A.
- Follow ECJ6 Mobility Office direction to manage device issue, turn-in, loss, damage, or security issues for organization on behalf of the user with Property Book Office (PBO) and USEUCOM Comptroller.

- Maintain records correlating the device's phone number, serial number, IMEI and SIM data to users and estimated commercial service billing expenses.
- Advise ODCs on procurement and life cycle replacement of USEUCOM supported CMDs based on ECJ6 Mobility Office guidance.

Office of Defense Cooperation (ODCs) and other remote locations in EUCOM's AOR countries, mostly in or near U.S. Embassies with approximately 40 remote sites.

ODC Site	# of Users	ODC Site	# of Users	ODC Site	# of Users
ALBANIA	7	GEORGIA	23	NORTH MACEDONIA	8
ARMENIA	7	GERMANY	10	NORWAY	6
AUSTRIA	2	GREECE	12	POLAND	16
AZERBAIJAN	7	HUNGARY	e	PORTUGAL	5
BOSNIA	9	IRELAND	1	ROMANIA	11
BRUSSELS/BELLUX	8	ISRAEL	9	SERBIA	6
BULGARIA	10	ITALY	18	SLOVAKIA	5
CROATIA	6	KOSOVO	6	SLOVENIA	5
CYPRUS	1	LATVIA	6	SPAIN	15
CZECH REPUBLIC	6	LITHUANIA	6	SWEDEN	2
DENMARK	5	MOLDOVA	8	SWITZERLAND	2
ESTONIA	6	MONTENEGRO	4	UKRAINE	41
FINLAND	4	NETHERLANDS	6	UNITED KINGDOM	7
FRANCE	7				

C.6.1.1.44. CYBERSECURITY HOST-BASED SECURITY SYSTEM SUPPORT [*EXERCISED FOR EUCOM*]

As a supplement to task C.5.2.2.22.1 CYBER SECURITY OPERATIONS, the Contractor shall provide Host-Based Security System support to EUCOM networks.

The Contractor shall:

- Operate and maintain systems required to support endpoint level security tools.
- Maintain EUCOM endpoint security tools In Accordance With (IAW) JFHQ OPORD 16-0080 FRAGO 6 and any subsequent FRAGO or replacement order as appropriate.
- Maintain EUCOM endpoint security posture IAW Cyber Command Readiness Inspection (CCRI) and Cybersecurity Service Provider (CSSP) evaluation scoring metric criteria.
- Maintain e-Policy Orchestrator (ePO) server(s) IAW minimum supported version as published in the DoD patch repository (https://patches.csd.disa.mil) and IAW applicable Security Technical Implementation Guidance (STIG) documents.
- Deploy required ESS products to EUCOM endpoints at or above minimum required patch levels including mandated antivirus products, intrusion detection / prevention products, data-loss prevention products, rogue detection products, and compliance detection / reporting products. Maintain current compliance metric of 95% properly implemented ESS coverage on a per product basis OR any updated requirement brought about through updated OPORDs, TASKORDs, or CTOs.
- Configure security tools to ensure correct compliance data is available during periodic reporting / rollup reporting to Continuous Monitoring and Risk Scoring (CMRS) or other required reporting location as required by OPORD / CCRI inspection criteria.
- Configure and assign point product policies to EUCOM endpoints IAW applicable STIGs.
- Tune assigned point product policies, maintain, and track exceptions required to remove false positives and known non-malicious behaviors.
- Monitor, report, and investigate unknown and potentially malicious detected activity.
- Performance tune assigned point product policies to minimize resource use without compromising effective security posture.

- Monitor ESS program for updated guidance and products. Test, integrate, and deploy new / updated products and policies within DoD specified timeframes.
- Maintain administrator training IAW CCRI specified requirements to properly manage the endpoint security suite.

C.6.1.2. GOVERNMENT DIRECTED OVERTIME/SURGE SUPPORT (OPTIONAL)

It is anticipated that the Government may require the Contractor to work overtime or surge resources to support additional Government 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 or exercised options for this Task Order. The Contracting Officer Representative (COR) will ensure sufficient funds exist to support the requirements prior to execution of support.

For proposal purposes, the Not-to-Exceed (NTE) value of this unburdened option is **$1,000,000** per year. The value of this option includes OT/Surge (Labor) support.

Typical examples of overtime/surge support that could be exercised include, but are not limited to:

- Exercise support when adjusting the normal work schedule; minimizing/prohibiting leave of individual contractor employees; adjusting service level agreements DOES NOT achieve the required coverage.
- Real World Operations when adjusting the normal work schedule; minimizing/prohibiting leave of individual contractor employees; adjusting service level agreements DOES NOT achieve the required coverage.
- Crashing project schedule(s) to achieve Government directed completion dates.
- Short term projects, as directed by the Government

Government directed overtime should only be used when all other possibilities have been exhausted. It should not be used to support normal maintenance such as outages requiring Contractor employees to work after hours or weekends. Overtime costs shall not be incurred unless authorized by the Contracting Officer (CO) or the Contracting Officer's Representative (COR) and unless funding is available to cover incurred expenses.

At the time of exercising this optional support, the Government will issue a Technical Direction Letter (TDL), which at a minimum shall include:

- Identify the event (exercise/operation/project) which is driving the overtime requirement.
- Identify the specific services where overtime or surge is authorized.
- 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.

Note: In limited circumstances, the Government may issue Technical Direction via email.

C.6.1.2.1. CONTINGENCY AND EXERCISE SURGE SUPPORT

Contingencies are typically unannounced and have an unknown duration. The Contractor may be required to surge current work force to meet 24x7 operational needs. As much as possible, this surge should be satisfied within existing staffing levels, and without degradation of service. However, if needed, the Contractor may request overtime and/or relief from service levels from the Government. Should

operations continue long enough the Government may require, or the Contractor may request, additional resource be brought in TDY to meet mission needs.

Exercise surges are planned events; therefore, although additional work may be required, there should be sufficient time to schedule the work to not impact current operations. Normally, exercise scenarios progress on a non-mission interference basis during normal duty hours. The Contractor shall coordinate with the Government to adjust staff schedules to support exercises while concurrently delivering ongoing day-to-day services and support within the available staffing levels. Where directed by the Government, the Contractor shall provide 24x7 coverage during the exercises. This may include adjusting the normal work schedule or minimizing/prohibiting leave of individual contractor employees to achieve the required coverage.

The Contractor will be expected to participate in all operational and exercise surges, consistent with the level of service specified by the CCMD. The CCMD will establish the specific requirements for extended hours of operation by technical support areas. Examples of tasks include:

- Configuring and deploying hardware to support the operation/exercise
- Establishing new or expanding existing network services
- Establishing new or expanding existing Operation Centers
- Troubleshooting and resolving network and user problems

C.6.1.2.2. PROJECT SURGE SUPPORT

Project surge support requires enhanced resources to support approved IT projects; for example, large lifecycle replacements and major transition of technologies. The requirement for this service is part of Government approved project documents.

(END OF SECTION C)

SECTION D – PACKAGING AND MARKING

NOTE: Section D of the Contractor's Basic GSA Alliant 2 GWAC is applicable to this Task Order and is hereby incorporated by reference. In addition, the following applies:

D.1. TASK ORDER DELIVERABLES/SUPPLIES

The Contractor shall provide electronic copies of each deliverable. Electronic copies shall be delivered via email attachment or other media/methods by mutual agreement of the parties.

D.2. DELIVERABLES MEDIA

The Contractor shall deliver all electronic versions of deliverables by email or other method as agreed, and place a copy in the client-designated deliverable repository. Identified below is the range of electronic deliverable types. The Contractor shall submit electronic deliverables in a format compatible with current MS Office versions of the specified software in use by the client.

- Text — Microsoft Word
- Spreadsheets — Microsoft Excel
- Briefings — Microsoft PowerPoint
- Drawings — Microsoft Visio
- Schedules — Microsoft Project

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

(END OF SECTION D)

SECTION E – INSPECTION AND ACCEPTANCE

NOTE: Section E of the Basic GSA Alliant 2 GWAC is applicable to this Task Order and is hereby incorporated by reference. In addition, the following applies:

E.1. PLACE OF INSPECTION AND ACCEPTANCE

Inspection of all work performance, reports, and other deliverables under this Task Order shall be performed by the Technical Points of Contact (TPOCs) designated in Section G.1.

Acceptance of all work performance, reports, and other deliverables under this Task Order shall be performed by the COR designated in Section G.1.

E.2. SCOPE OF INSPECTION

E.2.1. All deliverables will be inspected for content, completeness, accuracy and conformance to Task Order requirements by the COR. Inspection may include validation of information or software through the use of automated tools, testing or inspections of the deliverables, as specified in the Task Order. The scope and nature of this inspection will be sufficiently comprehensive to ensure the completeness, quality and adequacy of all deliverables.

E.2.2. The Government requires a period not to exceed fifteen (15) work days after receipt of final deliverable items for inspection and acceptance or rejection.

E.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 contract. Deliverable items rejected shall be corrected in accordance with the applicable clauses.

E.3.1. The final acceptance of deliverables will occur when all discrepancies, errors or other deficiencies identified in writing by the Government have been resolved, either through documentation updates, correction or other mutually agreeable methods.

E.3.2. Reports, documents and narrative type deliverables will be accepted when all discrepancies, errors or other deficiencies identified in writing by the Government have been corrected.

E.3.2.1. If the draft deliverable is adequate, the Government may accept the draft and provide comments for incorporation into the final version.

E.3.2.2. 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.

E.3.2.3. If the Government finds that a draft or final deliverable contains excessive spelling errors, grammatical errors, improper format, or otherwise does not conform to the requirements stated within this Task Order, the document may be immediately rejected without further review and returned to the Contractor for correction and resubmission. If the Contractor requires additional Government guidance to produce an acceptable draft, the Contractor shall arrange a meeting with the COR.

E.4. DRAFT DELIVERABLES

E.4.1. The Government will provide written acceptance, comments and/or change requests, if any, within ten (10) work days (unless specified otherwise in Section F) from Government receipt of the draft deliverable.

E.4.2. Upon receipt of the Government 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.

E.5. WRITTEN ACCEPTANCE/REJECTION BY THE GOVERNMENT

The Government shall provide written notification of acceptance or rejection of all final deliverables within ten (10) work days (unless specified otherwise in Section F). All notifications of rejection will be accompanied with an explanation of the specific deficiencies causing the rejection. If the Government does not respond within ten (10) work days receipt of a final work product from the Contractor, the product will be considered acceptable by the Government.

E.6. NON-CONFORMING PRODUCTS OR SERVICES

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

(END OF SECTION E)

SECTION F – DELIVERIES OR PERFORMANCE

NOTE: Section F of the Contractor's Basic GSA Alliant 2 GWAC is applicable to this Task Order and is hereby incorporated by reference. In addition, the following applies:

F.1. PLACE OF PERFORMANCE, DUTY HOURS, and HOLIDAYS

F.1.1. PLACE OF PERFORMANCE

Primary places of performance include:

- U.S. AFRICOM Headquarters at Kelley Barracks, Moehringen, Germany
- U.S. EUCOM Headquarters at Patch Barracks, Vaihingen, Germany
- Camp Lemonnier, Djibouti
- SHAPE, Mons, Belgium
- Caserma Del Din, Vicenza, Italy
- Pentagon Liaison Office, Arlington, VA
- Baledogle Military Airfield (BMA), Somalia
- Mogadishu Base Cluster (MOG), Somalia
- Manda Bay (Camp Simba), Kenya

The Contractor shall provide permanent staffing support at Kelley Barracks, Patch Barracks, Camp Lemonnier, SHAPE, Caserma Del Din, and the Pentagon. The Government may require temporary duty (travel) to the aforementioned locations as well as Garmisch, Germany; RAF Molesworth, UK; and other locations within the AFRICOM and EUCOM areas of responsibility (AOR).

F.1.2. CORE/DUTY HOURS

Normal core/duty hours for AFRICOM and EUCOM are Monday through Friday, excluding U.S. Holidays, from 0730 to 1630 which includes 1 hour for lunch; and there is a limited user presence throughout the night and on weekends. The Contractor shall staff accordingly.

Normal core/duty hours at Camp Lemonnier, Djibouti are Monday through Saturday, including most US Holidays, from 0730 to 1830 which includes 1 hour for lunch. The normal work week for personnel assigned to Camp Lemonnier is 6 days on and 1 day off or 60 hours per week. The Contractor shall staff accordingly.

F.1.3. HOLIDAYS

With the exception of CJTF-HOA, the following federal holidays are observed and therefore shall be staffed similar to other non-duty days (i.e. weekends):

New Year Day
Martin Luther King Day
President's Day
Memorial Day
Independence Day
Labor Day
Columbus Day
Veteran's Day
Thanksgiving Day
Christmas Day

Reduced staffing and/or partial workdays may be possible at CJTF-HOA during federal holidays with Government (TPOC) approval.

F.2. PERIOD OF PERFORMANCE

This task order consists of 3-month Transition Period, 12-month Base Period, and four (4) subsequent 12-months option periods, with an effective date, as follows:

- Base Year: 01 Jun 2019 through 31 May 2020 (Includes 90 day transition period)
- Option Year 1: 01 Jun 2020 through 31 May 2021
- Option Year 2: 01 Jun 2021 through 31 May 2022
- Option Year 3: 01 Jun 2022 through 31 May 2023
- Option Year 4: 01 Jun 2023 through 31 May 2024

The Government may extend the term of this task order by written notice to the contractor within 15 days of the expiration of the existing period of performance provided that a preliminary notice of the Government's intent to extend is provided at least 30 days before the expiration of the task order. The preliminary notice does not commit the Government to an extension. If the Government exercises this option, the extended task order shall be considered to include this option clause. The Government shall have the unilateral right to exercise options periods.

F.3. PLACE(s) OF DELIVERY

Unclassified deliverables and correspondence shall be delivered to the primary GSA Contracting Officer's Representative designated in Section G.1.

Copies of all deliverables (classified and unclassified) shall also be delivered to the designated TPOCs designated in Section G.1.

F.4. NOTICE REGARDING LATE DELIVERY/PROBLEM NOTIFICATION REPORT

The Contractor shall notify the COR via a Problem Notification Report (PNR) as soon as it becomes apparent to the Contractor, that a scheduled delivery will be late. The Contractor shall include in the PNR the rationale for late delivery, the expected date for the delivery and the project impact of the late delivery. The COR will review the new schedule and provide guidance to the Contractor. Such notification in no way limits any Government contractual rights or remedies including but not limited to termination.

F.5. DELIVERABLES SCHEDULE

The list of specific deliverables and schedule of milestones is included in PWS Section C.5.2.6.

(END OF SECTION F)

SECTION G - CONTRACT ADMINISTRATION DATA

NOTE: Section G of the Contractor's Basic GSA Alliant 2 GWAC is applicable to this Task Order and is hereby incorporated by reference. In addition, the following applies:

G.1. POINTS OF CONTACT

GSA Contracting Officer:

Alex Garcia
GSA FAS, Mid-Atlantic Region
100 South Independence Mall West
Philadelphia PA 19106
Office: 215-446-5868; Email: alexander.garcia@gsa.gov

On-Site GSA Contracting Officer:

Rahul Asher
Duty Station: USAG Stuttgart
Office (Patch Barracks): (b) (6)
~~Office (Kelley Barracks) :~~ (b) (6)
Email : rahul.asher@gsa.gov and (b) (6)

GSA Contracting Officer's Representative (COR):

GSA COR: Timothy Bowers
Duty Station: USAG Stuttgart
Office: (b) (6)
Email: timothy.bowers@gsa.gov and (b) (6)

GSA COR: Melissa Mould
Duty Station: USAG Stuttgart
~~Office (Patch Barracks):~~ (b) (6)
Office (Kelley Barracks) : (b) (6)
Email : melissa.mould@gsa.gov and (b) (6)

Technical Points of Contact (TPOCs) for the Client Agencies:

- USAFRICOM TPOC:
  To Be Designated ~~Upon Task Order Award~~ on a separate attachment titled USAFRICOM TPOC

- USEUCOM TPOC:
  To Be Designated ~~Upon Task Order Award~~ on a separate attachment titled USAFRICOM TPOC

- DJIBOUTI TPOC:
  To Be Designated ~~Upon Task Order Award~~ on a separate attachment titled USAFRICOM-CJTF-HOA TPOC

G.1.1. CONTRACTING OFFICER'S REPRESENTATIVE

The GSA Contracting Officer (CO) will appoint a GSA Contracting Officer's Representative (COR) in writing. The COR will receive, for the Government, all work called for by the TO and will represent the

CO in the technical phases of the work. The COR will provide no supervisory or instructional assistance to contractor personnel.

The COR is not authorized to change any of the terms and conditions of the Contract or the TO. Changes in the scope of work will be made only by the CO by properly executed modifications to the Contract or the TO.

G.1.2. TECHNICAL POINTS OF CONTACT

The Technical Points of Contact (TPOCs) listed under G.1 are responsible for providing technical direction and setting priorities in the operational areas of work performed under their purview.

TPOCs are not authorized to change any of the terms and conditions of the Contract or the TO. Changes in the scope of work will be made only by the CO by properly executed modifications to the Contract or the TO.

G.2. TECHNICAL DIRECTION

(a) Performance of the work under this task order shall be subject to the technical direction of the GSA Contracting Officer's Representative (COR). The term "technical direction" is defined to include, without limitation:

(1) Providing direction to the contractor that redirects contract effort, shift work emphasis between work areas or tasks, require pursuit of certain lines of inquiry, fill in details, or otherwise serve to accomplish the contractual Performance Work Statement.

(2) Providing written information to the contractor that assists in interpreting drawings, specifications, or technical portions of the work description.

(3) Reviewing and, where required by the contract, approving, technical reports, drawings, specifications, and technical information to be delivered by the contractor to the Government.

(b) The contractor will receive a copy of the written COR and Technical Point of Contact (TPOC) designation from the contracting officer. It will specify the extent of the COR's and TPOCs authority to act on behalf of the contracting officer.

(c) Technical direction must be within the scope of work stated in the contract. The COR and TPOC does not have the authority to, and may not, issue any technical direction that:

(1) Constitutes an assignment of additional work outside the Performance Work Statement;

(2) Constitutes a change as defined in the contract clause entitled "Changes;"

(3) In any manner causes an increase or decrease in the total estimated contract cost, the fee (if any), or the time required for contract performance;

(4) Changes any of the expressed terms, conditions or specifications of the contract; or

(5) Interferes with the contractor's right to perform the terms and conditions of the contract.

(d) All technical direction shall be issued in writing by the COR and TPOC.

(e) The contractor must proceed promptly with the performance of technical direction duly issued by the COR or TPOC in the manner prescribed by this clause and within its authority under the provisions of this clause. If, in the opinion of the contractor, any instruction or direction by the COR or TPOC falls within one of the categories defined in (c)(1) through (c)(5) of this clause, the contractor must not proceed and must notify the Contracting Officer in writing within five (5) working days after receipt of any such instruction or direction and must request the Contracting Officer to modify the contract accordingly. Upon receiving the notification from the contractor, the Contracting Officer must:

(1) Advise the contractor in writing within thirty (30) days after receipt of the contractor's letter that the technical direction is within the scope of the contract effort and does not constitute a change under the Changes clause of the contract;
(2) Advise the contractor in writing within a reasonable time that the Government will issue a written change order; or
(3) Advise the contractor in writing within a reasonable time not to proceed with the instruction or direction of the COR.

(f) A failure of the contractor and Contracting Officer either to agree that the technical direction is within the scope of the contract or to agree upon the contract action to be taken with respect to the technical direction will be subject to the provisions of the clause entitled "Disputes."

G.3. INVOICE SUBMISSION

The Contractor shall submit Requests for Payments in accordance with the format contained in GSAM 552.232-70, INVOICE REQUIREMENTS (SEPT 1999), to be considered proper for payment. In addition, the data elements indicated below shall be included on each invoice.

Task Order number: *(from GSA Form 300, Block 2)*
Paying Number: *(ACT/DAC NO.) (From GSA Form 300, Block 4)*
Project No.
Project Title

The Contractor shall provide invoice backup data in accordance with the contract type, including detail such as labor categories, rates and quantities of labor hours per labor category.

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

G.3.1. INVOICE REQUIREMENTS

The Contractor shall submit a draft or advance copy of an invoice to the client POC for review prior to its submission to GSA.

The Contractor shall invoice monthly on the basis of cost incurred for the Labor, Base Fee, Travel, Tools, and ODC CLINs. 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.

Content of Invoice: The Contractor's invoice shall be submitted monthly for work performed the prior month. The contractor may invoice only for the hours, travel, tools, ODCs, 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 Contract Number
2. Contract 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)

All hours and costs shall be reported by CLIN element (as shown in Section B) and contractor employee, and shall be provided for the current billing month and in total from project inception to date. The contractor shall provide the invoice data in a Microsoft Excel spreadsheet format containing separate worksheets showing the information. The invoice shall include the period of performance covered by the invoice and the CLIN numbers and titles. The Government reserves the right to modify invoicing requirements at its discretion. The contractor shall comply with any revised invoicing requirements at no additional cost to 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

Interim Close Outs: The Government will close each Performance Period at completion and will use Quick-Closeout Procedures in accordance with FAR 42.708 when possible. The contractor shall submit a final invoice within sixty (60) calendar days after the end of the each 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. The Contractor will be required to execute a waiver of claims to be included in a bi-lateral modification at the conclusion of the performance period.

Final Invoice: Invoices for final payment must be so identified and submitted within 6 months from task order completion. After this submission, no further charges are to be billed. A copy of the written client agency 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 6-month time frame.

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

Close-out Procedures: 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.

Charges:

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

Credits:

- 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.

- 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 COR 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:

a. 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.

G.3.1.1. FIRM FIXED PRICE (FFP) CLINS FOR LABOR

For FFP Labor CLINs, the Contractor shall invoice monthly on the basis of an equitable proportion of the fixed price costs allocable to the invoicing period. For example:

- For FFP CLINs with a 12-month performance period, monthly invoices shall reflect $1/12^{th}$ of the overall value of the FFP CLIN for the 12-month period.
- For FFP CLINs with a performance period of less than 12-months in duration, monthly invoices shall reflect $1/n^{th}$ of the overall value of the FFP CLIN, where n = the total number of months in the performance period.

G.3.1.2. COST PLUS FIXED FEE (CPFF) TERM CLINS FOR LABOR

The Contractor shall invoice monthly on the basis of cost incurred for the CPFF Labor CLINs. All hours and costs shall be reported by CLIN element (as shown in Section B) and contractor employee, and shall be provided for the current billing month and in total from project inception to date. The Contractor shall provide the invoice data on separate worksheets in spreadsheet form with the following detailed

information. The listing shall include separate columns and totals for the current invoice period and the project to date.

- Employee name (current and past employees)
- Employee company labor category
- Employee Alliant labor category and Associated Skill Level
- Actual Hours worked during the monthly billing period and total cumulative hours worked
- Billing rate

All cost presentations provided by the Contractor shall also include Overhead Charges, and General and Administrative Charges clearly shown both as a percentage and total dollars.

Fee: The contractor's monthly invoice shall include the current and cumulative Fixed Fee. The monthly fixed fee invoiced shall be proportionate to the labor (dollars) expended for the month invoiced. When the work required under any CLIN is completed, and that work is within the total estimated cost shown in Section B (funded amount provided in ASSIST), the contractor shall be entitled to payment of fixed fee proportional to cost incurred for that CLIN. The contractor may present, with its monthly vouchers for costs, a fee voucher in an amount bearing the same percentage of fixed fee as the certification of incurred costs bears to the total estimated cost for each CLIN. However, in accordance with FAR 52.216-8, after payment of 85 percent of the fixed fee for the total Task Order, the Contracting Officer may withhold further payment of fixed fee until a reserve shall have been set aside in an amount which the Contracting Officer considers necessary to protect the interest of the Government. This reserve shall not exceed 15 percent of the total fixed fee or $100,000, whichever is less.

Federal Acquisition Regulation (FAR) Clause 52.232-22, Limitation of Funds, applies to this Task Order on a CLIN-by-CLIN basis.

G.3.1.3. TRAVEL

Costs incurred for Travel comparable with the FTR, JTR, and DSSR shall be invoiced monthly with travel itemized by Individual and Trip. The Contractor shall adhere to FAR part 31.205-46 for travel associated with this contract. This shall include all travel requirements associated with temporary duty (TDY) or deployments as required under this task order, Contractor personnel are authorized to invoice travel related costs at the allowance referenced in FAR part 31.205-46. The Contractor shall provide the Travel invoice data on separate worksheets in Microsoft Excel spreadsheet form with the following detailed information.

The invoice information shall identify all cumulative travel costs billed by CLIN. Cost incurred for Travel shall be shown on the monthly invoice with travel itemized by individual and trip. The Contractor shall provide travel invoice data on separate worksheets in Microsoft Excel spreadsheet format with the following details. The current invoice period's travel detail shall include separate columns and totals and include the following:

- Travel Authorization Request Number or identifier
- Current invoice period
- Names of persons traveling
- Number of travel days
- Dates of travel
- Location of travel
- Number of days per diem charged

- Per diem rate used
- Total per diem charged
- Transportation costs
- Total charges

All cost presentations provided by the contractor shall include Overhead Charges and General and Administrative Charges. Fee shall not be permitted on travel costs.

G.3.1.4. TOOLS AND ODCS

Costs incurred for the Tools and ODC CLINs shall be invoiced monthly and be itemized. The Contractor shall provide the Tools/ODC invoice data on separate worksheets in Microsoft Excel spreadsheet form with the following detailed information, as applicable:

- Tools purchased and/or ODC costs incurred
- Consent to Purchase Number or identifier
- Description of the Tools with the Quantity, Unit Price and Extended Price of each Tool and/or ODC identified
- Ship To Location(s) and Date(s) accepted by the Government
- Associated CLINs
- Project to date totals by CLIN
- Cost incurred not billed
- Remaining balance of the associated CLINs

All cost presentations provided by the contractor shall also include Overhead Charges, General and Administrative Charges, and or material handling as appropriate and consistent with DCAA recommendations. Feel shall not be permitted on Tools and ODC costs.

G.3.1.5. INDIRECT AND MATERIAL HANDLING RATE

Travel, ODCs, and incidentals incurred may be burdened with the Contractor's indirect/material handling rate consistent with the Contractor's proposal. Any proposed indirect or material handling rates proposed and invoiced shall be consistent with the Contractor's most recent Defense Contract Audit Agency (DCAA) rate approval or provisional rate letter. Offerors are advised that they will not be permitted to apply a burden rate of any kind to travel, ODCs, or incidental costs after award except to the extent that application of such burden is consistent with their proposal.

(END OF SECTION G)

SECTION H – SPECIAL CONTRACT REQUIREMENTS

NOTE: Section H of the Contractor's Basic GSA Alliant 2 GWAC is applicable to this Task Order and is hereby incorporated by reference. In addition, the following applies:

H.1. GOVERNMENT FURNISHED PROPERTY (GFP)

The current USAFRICOM/USEUCOM automated tools and systems shall be made available to the Contractor for use in the performance of this requirement.

The Government will provide Contractor personnel access to Government workspace including a desk, network access, telephone access, and electronic mail.

H.1.1. GOVERNMENT FURNISHED INFORMATION (GFI)

The Government will provide to the Contractor relevant systems documentation and all current documented policies and procedures.

H.2. TRAVEL

H.2.1. TRAVEL REGULATIONS

The Contractor shall adhere to the following travel regulations (see FAR 31.205-46):

(1) Federal Travel Regulations (FTR) – prescribed by the General Services Administration, for travel in the contiguous United States.
(2) Joint Travel Regulation (JTR) – prescribed by the Defense Travel Management Office
(3) Department of State Standardized Regulations (DSSR) (Government Civilians, Foreign Areas), Section 925, "Maximum Travel Per Diem Allowances for Foreign Areas", prescribed by the Department of State, for travel in areas not covered in the FTR or JTR.

H.2.2. TRAVEL AUTHORIZATION REQUESTS

Before undertaking travel to any Government site or any other site in performance of this Task Order, the Contractor shall have this travel approved by, and coordinated with, the COR. The Contractor shall notify the COR prior to any anticipated travel. Notification shall include, at a minimum, the number of persons in the party, traveler name, destination, duration of stay, purpose, and estimated cost. Prior to any long distance travel, the Contractor shall prepare a Travel Authorization Request for Government review and approval. The Government shall approve all travel in writing. Long distance travel will be reimbursed for cost of travel comparable with the FTR, JTR, and DSSR.

Requests for travel approval shall:

- Be prepared in a legible manner;
- Include a description of the travel proposed including a statement as to purpose;
- Be summarized by traveler;
- Identify the travel request/travel authorization number associated with the travel;
- Be submitted in advance of the travel with sufficient time to permit review and approval.
- Not be considered approved until written approval is received from the COR (email shall suffice in limited circumstances).

The Contractor shall propose and utilize an organized method and format for the tracking and approval process associated with Travel Authorization Requests to be reviewed and approved by the COR post award.

The Contractor shall use only the minimum number of travelers and rental cars needed to accomplish the task(s). Travel shall be scheduled during normal duty hours whenever possible.

H.2.3. TRIP REPORTS

The Government will identify the need for a Trip Report (if required) when the request for travel is submitted. The Contractor shall keep a summary of all long-distance travel, to include, at a minimum, the name of the employee, location of travel, duration of trip, and POC at travel location.

H.2.4. TOOLS - HARDWARE/SOFTWARE AND MISCELLANEOUS ODCs

The Government may require the Contractor to purchase hardware, software, and related items that are necessary and ancillary to the services being acquired under the TO. Such requirements will be identified at the time of award, or may be identified during the course of a TO, by the Government or the Contractor. If the Contractor initiates a purchase within the scope of this TO and the prime Contractor has an approved purchasing system, the Contractor shall submit a Request to Initiate Purchase (RIP) to the COR. If the prime Contractor does not have an approved purchasing system, the Contractor shall submit to the CO a Consent to Purchase (CTP). The RIP and CTP shall include the purpose, specific items, estimated cost, cost comparison to show competitive basis for fair and reasonable price determination, and rationale. The Contractor shall not make any purchases without a written approved RIP from the COR or a written approved CTP from the CO. Email approvals are authorized in limited circumstances.

H.3. SECURITY REQUIREMENTS

H.3.1. DD254 CONTRACT SECURITY CLASSIFICATION SPECIFICATION

The Government will furnish a DD Form 254 Contract Security Classification Specification at time of award (The DD254 is contained in Appendix G). The Contractor shall have a TOP SECRET Facility Clearance with NO Safeguarding requirement. The Contractor shall require access to COMSEC information, Sensitive Compartmented Information (SCI), Non-SCI information, NATO information and For Official Use Only (FOUO) information. The Contractor shall require access to the SIPRNET, JWICS and other classified systems as identified on the DD 254. The Contractor shall have access to classified materials at Government facilities only (OCONUS). The Contractor shall have OPSEC requirements.

H.3.2. SECURITY PLAN

The Contactor shall develop a written plan for physical security, document and material security, and personnel security IAW DoD, CCMDs, and local physical security regulations. The Government will review and approve this plan, and any subsequent changes to it. The Physical Security Plan shall include all GFP provided under this task order, and shall include: Receiving, storing, disseminating, transporting, and protecting items involved in the performance of this task order and classified by the Government as Confidential, Secret, Top Secret, or Sensitive Compartmented Information (SCI). This data or information will be processed IAW DoD 5220.22-R (Industrial Security Regulation (ISR)) and DoD 5200-22-M (National Industrial Security Program Operating Manual (NISPOM)).

Army Regulation 25-2 Information Management: Information Assurance: Section V Personnel Security; para. 4-14 Personnel Security Standards will be applied to all IT and IT-related positions, whether occupied

by DA civilian employees, military personnel, consultants, contractor personnel, or others affiliated with the DoD. Additional guidance is available in DoD 5200.2–R.

Personnel requiring access to information systems to fulfill their duties must possess the required favorable security investigation, security clearance, or formal access approvals, and fulfill any need-to-know requirements. AR 25-2 uses the designations of IT-I, IT-II, IT-III, and IT-IV which are defined based upon the role performed and the classification of the information system. Most contractor personnel on this contract will require the IA-I designation based upon their privilege access to systems and devices on the SIPR Network. Please see the referenced Section in AR 25-2 for more information and security clearance requirements. At minimum, all Contractor personnel shall have a fully adjudicated SECRET Clearance.

In addition to the requirements of AR 25-2, many of end users requiring support are located in Secure Compartmented Information (SCI) Facilities (SCIFs) which require a Top Secret/SCI security clearance to access. The Contractor shall have sufficient personnel cleared so that work in these areas can be accomplished unimpeded.

For positions identified as IT – II and III, foreign nationals may be appointed if they possess a unique or unusual skill or expertise that is urgently needed for a specific DoD requirement and for which a suitable United States citizen is not available, and approved in writing by the AFRICOM or EUCOM DAA.

The Government retains the right to request removal of contractor personnel, regardless of prior clearance or adjudication status, whose actions while assigned to this task order conflict with the interests of the Government. The reason for removal will be fully documented in writing by the Contracting Officer's Representative (COR) in coordination with the TPOC.

All contractor personnel are required, prior to being granted access to AFRICOM and EUCOM networks and/or systems, to obtain the proper security clearances, read and sign the User Agreement, and attend a Security Briefing (SIPR Access Only). Additionally, all contractor personnel assigned to IA-I and IA-II functions shall have DD Form 2875 System Authorization Access Request completed and approved prior to receiving privileged access.

The Contractor shall clearly show in their proposed Staffing Matrix the IT level and target security clearance level for each position. It shall be noted that all contractors to begin performance must possess at least a secret level security clearance.

H.4. CONTRACTOR PERSONNEL

Throughout the performance of this task order, the Contractor shall provide and maintain qualified personnel that have the requisite technical skills, qualifications, and experience together with the supervision, management and administrative services necessary to successfully meet the Government's requirements. The Contractor shall provide personnel, who are fully qualified and competent to perform their assigned work.

H.4.1. KEY PERSONNEL

Key personnel must be assigned for the duration of the Task Order, and may be replaced or removed subject to procedures in Section H.4.2 KEY PERSONNEL SUBSTITUTION below.

The Government has defined the following mandatory key personnel positions that are required for performance of this Task Order:

- Program Manager
- EUCOM Site Lead
- AFRICOM Site Lead
- CJTF-HOA Site Lead

H.4.1.1. PROGRAM MANAGER (KEY)

The Contractor shall name a Program Manager (PM) to serve as the Government's single program focal point with responsibility and authority for directing and managing contractor performance under this task order.

H.4.1.2. SITE LEADS (KEY)

The Contractor shall name a Site Lead for EUCOM, AFRICOM and CJTF-HOA to serve as the Government's central point-of-contact for each of the command's day-to-day operational activities and to provide the necessary technical direction, guidance and supervision for contractor personnel assigned to the task order.

The Contractor's PM/Site Leads should be able to demonstrate the following knowledge and/or experience:

- Understanding of operational and technical requirements of this Task Order.
- Understanding of applications and network systems similar to those in use at HQ USEUCOM and HQ USAFRICOM.
- Excellent written and verbal communication skills, and experience in presenting material to senior DoD and non-DoD officials
- Managerial experience in a C4 networking environment with a significant number of direct staff.
- Experience supervising substantial DoD C4 operations which encompass software development, user and network systems integration, and training in diverse operating environments with people of various job categories and skills.
- Experience in a quality assurance environment that includes, at a minimum, knowledge of: customer satisfaction tracking; user complaint and monitoring programs; and quality control (QC) systems reviews and analysis.
- Proven skills in manpower utilization, procurement, training, problem resolution, and employee relations.
- C4 experience in a military headquarters or command center environment.

H.4.2. KEY PERSONNEL SUBSTITUTION

The Contractor shall not remove or replace any personnel designated as key personnel under this TO without the written concurrence of the CO. Prior to utilizing other than personnel specified in the proposal submitted in response to this requirement, the Contractor shall notify the Government CO and the COR. This notification shall be no later than ten (10) calendar days in advance of any proposed substitution and shall include a resume for the proposed substitution and justification in sufficient detail to permit evaluation of the impact of the change on TO performance.

If the Government CO and the COR determine that the proposed substitute personnel is unacceptable, or that the reduction of effort would be so substantial as to impair the successful performance of the work under the TO, the substitution will be denied and the Contractor shall propose an alternate candidate.

H.5. PERSONNEL QUALIFICATIONS

IAW DoD 8570.01-M entitled "Information Assurance Workforce Improvement Program" requires all individuals performing Information Assurance functions to be certified appropriate to the position. Information Assurance functions includes all personnel with "elevated privileges" on the network and personnel who perform IA management functions. DoD 8570.01-M further stipulates that "Contractor personnel…shall obtain the appropriate DoD-approved IA baseline certification, prior to being engaged. Contractors have up to 6 months to obtain the rest of the qualifications for their position". For the purpose of this contract "the rest of the qualifications" is defined as Computer Environment qualifications.

The Contractor shall maintain certification for all IA positions in accordance with DoD Regulation 8570.01M and adhere to the Army 8570 tracking process (currently ATCTS) or other systems as designated by the Government to track contractor qualifications.

For all positions that fall under the IA Workforce Improvement Program, the Contractor shall provide a Staffing Matrix semi-annually. Additionally, the Government may request an updated Matrix when needed for Cyber Inspections such as a CCRI or CSSP inspection. The Staffing Matrix shall clearly show the following information:

- Employee's Name
- AR 25-2 IT level designation
- Task Area(s) Supported
- IA Workforce Category
- Baseline Certification
- Computer Environment Certification(s)*

*Not to exceed 3 shown in descending order of time spent in each Computing Environment

H.6. ORGANIZATIONAL CONFLICT OF INTEREST AND NON-DISCLOSURE REQUIREMENTS

H.6.1. ORGANIZATIONAL CONFLICT OF INTEREST

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

H.6.2. NON DISCLOSURE REQUIREMENTS

All Contractor personnel (to include Subcontractors, teaming partners, and consultants) who will be personally and substantially involved in the performance of the TO issued which requires the Contractor to act on behalf of, or provide advice with respect to any phase of an agency procurement, as defined in FAR 3.104-4, shall execute and submit an "Employee/Contractor Non-Disclosure Agreement" Form (See Section J, Attachment F). See FAR 3.104, discussing requirements for disclosure, protection, and marking of Contractor bid or proposal information, or source selection information. All Contractor personnel must submit a Non-Disclosure Agreement prior to the commencement of any work on the task order. Further, Contractor personnel must submit a Non-Disclosure agreement whenever replacement personnel are

proposed. Any information provided by Contractors in the performance of this TO or obtained by the Government is only to be used in the performance of the TO.

H.7. CONTRACTOR'S PURCHASING SYSTEMS

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

As part of the evaluation for task order award, the Contracting Officer shall verify the validity of the Contractor's purchasing system. Thereafter, the Contractor is required to certify to the Contracting Officer no later than (30) days prior to the exercise of any options the validity of their purchasing system. Additionally, if reviews are conducted of the purchasing system after the exercise of the option, the Contractor shall provide the results of the review to the Contracting Officer within two weeks from the date the results are known to the Contractor.

H.8. TRANSFER OF HARDWARE/SOFTWARE MAINTENANCE AGREEMENTS

If the Contractor acquires hardware/software maintenance support, all licenses and/or contractual rights to receive title shall be turned over to the Government upon completion of the task order.

The Government's liability to reimburse the Contractor for costs incurred from the acquisition of hardware/software maintenance support shall be limited to costs incurred during the period of the order for which the Government received the hardware/software maintenance support acquired by the Contractor on a cost reimbursable, no fee basis.

H.9. ASSOCIATE CONTRACTOR CONSIDERATIONS

There are functions within the scope of this Task Order where the Contractor must cooperate, share information, or otherwise jointly collaborate in the accomplishment of the government's requirements with other associate contractors working on separate government contracts. Where such contractor-to-contractor interfaces arise, the contractor is expected to establish professional, collaborative relationships with associate contractors to ensure the greatest degree of cooperation in providing technical solutions and services to successfully support mission needs within required time and cost constraints.

H.10. THEATER EXPERT STATUS ACCREDITATION (TESA) AND TECHNICAL REPRESENTATIVE (TR)

The Contractor shall be responsible for understanding and complying with DoD Contractor Personnel Office (DOCPER) TESA and TR requirements. The Contractor shall submit completed TESA and TR documentation to the GSA COR including: contract notification form, job descriptions, employee TESA applications, employee resumes, and employee employment contracts. After review and approval the GSA COR will submit all TESA and TR documents to DOCPER for approval.

The Government will assist the Contractor in coordination with SOFA agreements for countries in which performance is required under this Task Order.

Note: DOCPER information and resources can be obtained at:
http://www.eur.army.mil/g1/content/CPD/docper.html

(END OF SECTION H)

PART II – CONTRACT CLAUSES

SECTION I - CONTRACT CLAUSES

NOTE: In accordance with Section I of the Contractor's Basic GSA Alliant 2 Unrestricted GWAC, all applicable and required provisions and clauses set forth in FAR 52.301, Master Contract Section I.2, and Master Contract Section J - Attachment J-1 DoD Required Provisions and Clauses - automatically flow down to this task order as applicable. The table below incorporates clauses and provisions by reference, with the same force and effect as if they were given in full text. The full text may be accessed electronically at: https://www.acquisition.gov/far

In addition, the following applies:

I.1. FEDERAL ACQUISITION REGULATION (FAR) CLAUSES INCORPORATED BY REFERENCE

CLAUSE NO.	CLAUSE TITLE	DATE
52.217.5	Evaluation of Options	(JUL 1990)
52.227-01	Authorization and Consent	(Dec 2007)
52.227-02	Notice and Assistance Regarding Patent and Copyright Infringement	(Dec. 2007)
52.227-03	Patent Indemnity	(Apr 1984)
52.229-8	Taxes – Foreign Cost-Reimbursement Contracts	(MAR 1990)
52.232-39	Unenforcebility of Unauthorized Obligations	(JUN 2013)
52.237-1	Site Visit	(APR 1984)
52.237-3	Continuity of Services	(Jan 1991)
52.204-25	Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment	(Aug 2019)
52.211-15	Defense Priority and Allocation Requirements	(Apr 2008)

I.2. 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.

(End of clause)

I.3. 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 60 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 63 months.

(End of clause)

I.4. DEFENSE FEDERAL ACQUISITION REGULATION SUPPLEMENTS (DFARS) CLAUSES INCORPORATED BY REFERENCE

The table below incorporates clauses by reference, with the same force and effect as if they were given in full text.

The full text may be accessed electronically at: http://www.acq.osd.mil/dpap/dars/dfarspgi/current/

CLAUSE NO.	CLAUSE TITLE	DATE
252.204-7008	COMPLIANCE WITH SAFEGUARDING COVERED DEFENSE INFORMATION CONTROLS	(OCT 2016)
252.204-7009	LIMITATIONS ON THE USE OR DISCLOSURE OF THIRD-PARTY CONTRACTOR REPORTED CYBER INCIDENT INFORMATION	(OCT 2016)
252.225-7040	CONTRACTOR PERSONNEL SUPPORTING U.S. ARMED FORCES DEPLOYED OUTSIDE THE UNITED STATES	(OCT 2015)
252.225-7043	ANTITERRORISM/FORCE PROTECTION FOR DEFENSE CONTRACTORS OUTSIDE THE UNITED STATES	(JUN 2015)
252.225-7980	CONTRACTOR PERSONNEL PERFORMING IN THE UNITED STATES AFRICA COMMAND AREA OF RESPONSIBILITY (DEVIATION 2016-O0008)	(JUN 2016)
252.227-7013	RIGHTS IN TECHNICAL DATA - NONCOMMERCIAL ITEMS	(FEB 2014)
252.227-7014	RIGHTS IN NONCOMMERCIAL COMPUTER SOFTWARE AND NONCOMMERCIAL COMPUTER SOFTWARE DOCUMENTATION	(FEB 2014)
252.227-7015	TECHNICAL DATA—COMMERCIAL ITEMS	(FEB 2014)
252.227-7016	RIGHTS IN BID OR PROPOSAL INFORMATION	(JUN 2011)
252.227-7017	IDENTIFICATION AND ASSERTION OF USE, RELEASE, OR DISCLOSURE RESTRICTIONS	(JAN 2011)
252.227-7019	VALIDATION OF ASSERTED RESTRICTIONS - COMPUTER SOFTWARE	(SEP 2016)
252.227-7025	LIMITATIONS ON THE USE OR DISCLOSURE OF GOVERNMENT-FURNISHED INFORMATION MARKED WITH RESTRICTIVE LEGENDS	(MAY 2013)
252.227-7027	DEFERRED ORDERING OF TECHNICAL DATA OR COMPUTER SOFTWARE	(APR 1988)

252.227-7028	TECHNICAL DATA OR COMPUTER SOFTWARE PREVIOUSLY DELIVERED TO THE GOVERNMENT	(JUN 1995)
252.227-7037	VALIDATION OF RESTRICTIVE MARKINGS ON TECHNICAL DATA	(SEP 2016)
252.228-7003	CAPTURE AND DETENTION	(DEC 1991)
252.229-7002	CUSTOMS EXEMPTIONS (GERMANY)	(JUN 1997)
252.233-7001	CHOICE OF LAW (OVERSEAS)	(JUN 1997)
252.246-7001	WARRANTY OF DATA	(MAR 2014)
252.237-7023	CONTINUATION OF ESSENTIAL CONTRACTOR SERVICES	(OCT 2010)
252.237-7024	NOTICE OF CONTINUATION OF ESSENTIAL CONTRACTOR SERVICES	(OCT 2010)

I.4.1 DFARS Clause Fill-ins

252.237-7023 CONTINUATION OF ESSENTIAL CONTRACTOR SERVICES

(a) Definitions. As used in this clause—

(1) "Essential contractor service" means a service provided by a firm or individual under contract to DoD to support mission-essential functions, such as support of vital systems, including ships owned, leased, or operated in support of military missions or roles at sea; associated support activities, including installation, garrison, and base support services; and similar services provided to foreign military sales customers under the Security Assistance Program. Services are essential if the effectiveness of defense systems or operations has the potential to be seriously impaired by the interruption of these services, as determined by the appropriate functional commander or civilian equivalent.

(2) "Mission-essential functions" means those organizational activities that must be performed under all circumstances to achieve DoD component missions or responsibilities, as determined by the appropriate functional commander or civilian equivalent. Failure to perform or sustain these functions would significantly affect DoD's ability to provide vital services or exercise authority, direction, and control.

(b) The Government has identified all or a portion of the contractor services performed under this contract as essential contractor services in support of mission essential functions. These services are listed in attachment N, Mission-Essential Contractor Services, dated 17 March 2020.

(c)(1) The Mission-Essential Contractor Services Plan submitted by the Contractor, is incorporated in this contract.

(2) The Contractor shall maintain and update its plan as necessary. The Contractor shall provide all plan updates to the Contracting Officer for approval.

(3) As directed by the Contracting Officer, the Contractor shall participate in training events, exercises, and drills associated with Government efforts to test the effectiveness of continuity of operations procedures and practices.

(d)(1) Notwithstanding any other clause of this contract, the contractor shall be responsible to perform those services identified as essential contractor services during crisis situations (as directed by the Contracting Officer), in accordance with its Mission-Essential Contractor Services Plan.

(2) In the event the Contractor anticipates not being able to perform any of the essential contractor services identified in accordance with paragraph (b) of this section during a crisis situation, the Contractor shall notify the Contracting Officer or other designated representative as expeditiously as possible and use its best efforts to cooperate with the Government in the Government's efforts to maintain the continuity of operations.

(e) The Government reserves the right in such crisis situations to use Federal employees, military personnel or contract support from other contractors, or to enter into new contracts for essential contractor services.

(f) Changes. The Contractor shall segregate and separately identify all costs incurred in continuing performance of essential services in a crisis situation. The Contractor shall notify the Contracting Officer of an increase or decrease in costs within ninety days after continued performance has been directed by the Contracting Officer, or within any additional period that the Contracting Officer approves in writing, but not later than the date of final payment under the contract. The Contractor's notice shall include the Contractor's proposal for an equitable adjustment and any data supporting the increase or decrease in the form prescribed by the Contracting Officer. The parties shall negotiate an equitable price adjustment to the contract price, delivery schedule, or both as soon as is practicable after receipt of the Contractor's proposal.

(g) The Contractor shall include the substance of this clause, including this paragraph (g), in subcontracts for the essential services.

(End of clause)

252.237-7024 NOTICE OF CONTINUATION OF ESSENTIAL CONTRACTOR SERVICES

(a) Definitions. "Essential contractor service" and "mission-essential functions" have the meanings given in the clause at 252.237-7023, Continuation of Essential Contractor Services, in this solicitation.

(b) The offeror shall provide with its offer a written plan describing how it will continue to perform the essential contractor services listed in attachment N, Mission-Essential Contractor Services, dated 17 March 2020, during periods of crisis. The offeror shall–

(1) Identify provisions made for the acquisition of essential personnel and resources, if necessary, for continuity of operations for up to 30 days or until normal operations can be resumed;

(2) Address in the plan, at a minimum—

(i) Challenges associated with maintaining essential contractor services during an extended event, such as a pandemic that occurs in repeated waves;

(ii) The time lapse associated with the initiation of the acquisition of essential personnel and resources and their actual availability on site;

(iii) The components, processes, and requirements for the identification, training, and preparedness of personnel who are capable of relocating to alternate facilities or performing work from home;

(iv) Any established alert and notification procedures for mobilizing identified "essential contractor service" personnel; and

(v) The approach for communicating expectations to contractor employees regarding their roles and responsibilities during a crisis.

(End of clause)

I.5. CONTRACTOR MANPOWER REPORTING (CMR)

Contractor Manpower Reporting (CMR) is required via Army Regulation 25-2 to support the Assistant Secretary of the Army, Manpower and Reserve Affairs (ASA-M&RA) initiative to provide improved visibility to the contractor service workforce from contractors supporting the Army.

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 contract. The contractor is required to completely fill in all the information in the format using the following web address; https://www.ecmra.mil/. The required information includes:

(1) Contracting Office, Contracting Officer, Contracting Officer's Technical Representative;
(2) Contract number, including task and delivery order number;
(3) Beginning and ending dates covered by reporting period;
(4) Contractor name, address, phone number, email address, identity of contractor employee entering data;
(5) Estimate direct labor hours (including sub-contractors);
(6) Estimated direct labor dollars paid this reporting period (including sub-contractors);
(7) Total payments (including sub-contractors);
(8) Predominant Federal Service Code (FSC) reflecting services provided by contractor (and separate predominant FSC for each sub-contractor if different);
(9) Estimated data collection cost;
(10) Organizational title associated with the Unit Identification Code (UIC) for the Army Requiring Activity (the Army Requiring Activity is responsible for providing the contractor with its UIC for the Purposes of reporting this information);
(11) Locations where contractor and sub-contractors perform the work (specified by zip code in the United States and nearest city, country, when in an overseas location, using standardized nomenclature provided on website);
(12) Presence of deployment or contingency contract language; and

(13) Number of contractor and sum-contractor employees deployed in theater this reporting period (by country).

As part of its submission, the contractor will also provide the estimated total cost (if any) incurred to comply with this reporting requirement. Reporting period will be the period of performance not to exceed 12 months ending 30 September of each government fiscal year and must be reported by 31 October of each calendar year. Contractors may use a direct XML data transfer to the database server or fill in the fields on the website. The XML direct transfer is a format for transferring files from a contractor's systems to the secure web site without the need for separate data entries for each required data element at the web site. The specific formats for the XML direct transfer may be downloaded from the web site.

(End of provision)

I.6. SECTION 508 COMPLIANCE

Unless the Government invokes an exemption, all EIT products and services proposed shall fully comply with Section 508 of the Rehabilitation Act of 1973, per the 1998 Amendments, and the Architectural and Transportation Barriers Compliance Board's Electronic and Information Technology Accessibility Standards at 36 CFR 1194. The Contractor shall identify all EIT products and services proposed, identify the technical standards applicable to all products and services proposed and state the degree of compliance with the applicable standards. Additionally, the Contractor must clearly indicate where the information pertaining to Section 508 compliance can be found (e.g., Vendor's or other exact web page location). The Contractor must ensure that the list is easily accessible by typical users beginning at time of award.

The Contractor must ensure that all EIT products and services proposed that are less than fully compliant, are offered pursuant to extensive market research, which ensures that they are the most compliant products available to satisfy the solicitation's requirements.

If any such EIT product or service proposed is not fully compliant with all of the standards, the Contractor shall specify each specific standard that is not met; provide a detailed description as to how the EIT product or service does not comply with the identified standard(s); and shall also indicate the degree of compliance.

(END OF SECTION I)

SECTION J – LIST OF DOCUMENTS, EXHIBITS, AND OTHER ATTACHMENTS

NOTE: Section J of the Basic GSA Alliant 2 GWAC is applicable to this Task Order and is hereby incorporated by reference. In addition, the following applies:

The information provided in Section J is for reference purposes. The reference documents are not intended to change the TO and any conflict therein should be resolved by referring to and relying upon the TO. Because the reference materials may be outdated or contain information that has not been recently verified for accuracy, the Government does not warrant the accuracy of the information for purposes of this TO, and reserves the right to incorporate updated versions of any and all appendices at any time, and from time to time at its sole discretion. Updated versions of appendices shall be incorporated at no additional cost to the Government.

J.1. LIST OF ATTACHMENTS

Attachments furnished with the Task Order are "For Official Use Only"

Attachment	Description	For Reference Purposes Only
A	Specific Governing Directives	x
B	Requirements Alignment Matrix Amd 07	
C	USAFRICOM Documents: (1) AFRICOM C4 Systems Overview (2) AFRICOM Approved SW List (3) AFRICOM Approved HW List (4) AFRICOM Primary Hand Receipt (5) AFRICOM CJTF-HOA Hand Receipt (6) AFRICOM IPTV Connectivity (7) AFRICOM J65 Projects & Tasks (8) AFRICOM Exercise Support Data (9) AFRICOM CJTF-HOA Device Counts (10) AFRICOM CJTF-HOA Network Diagrams (11) AFRICOM NIPR Diagram (12) AFRICOM SIPR Diagram (a & b) (13) AFRICOM Device Counts	
D	USEUCOM Documents: (1) EUCOM C4 Systems Overview (2) EUCOM NIPR Diagram (3) EUCOM SIPR Diagram (4) EUCOM SEAGULL Network Diagram (5) EUCOM CSfC Network Diagram (6) EUCOM SWA Network Diagram (7) EUCOM GCTF Network Diagram (8) EUCOM IPTV Network Diagram (9) EUCOM EMCC ThinkLogical Network Diagram (10) EUCOM Software APL (11) EUCOM Hardware APL (12) EUCOM Standard Baseline Software	

	(13) EUCOM Operational Hand Receipt (14) EUCOM Warehouse Hand Receipt (15) EUCOM J6 Prioritized Projects (16) EUCOM Exercise Support Data (17) EUCOM JRSS JMN Permissions Matrix	
E	CJTF-HOA Documents: (1) AFRICOM General Order No. 1 (2) U.S. Djibouti Access Agreement (3) AFRICOM Theater Entry Summary Guide (4) Djibouti Airport Entry-Exit Procedures & Visa Fees (5) Camp Lemonnier Orientation Map (6) Camp Lemmonier Liberty Map (Includes a & b) (7) Camp Lemonnier Djibouti Housing Market Study	x
F	Contractor Non-Disclosure Agreement (Sample)	x
G	DD Form 254 (Draft)	
H	Logistical Support Annex: (1) Logistical Support Annex – Europe (2) Logistical Support Annex – CJTF-HOA	
I	Quality Assurance Surveillance Plan (QASP)	
J	Performance Requirements Summary (PRS)	
K	Monthly Status Reports – Redacted: (1) Mar 2018 MSR Redacted (2) April 2018 MSR Redacted (3) May 2018 MSR Redacted	x
L	Call Center Call Summary	x
M	Funding Summary Table (To be provided post award)	
N	Mission Essential Requirements	

(END OF SECTION J)