United States Special Operations Command (USSOCOM) Enterprise Operations and Maintenance (O&M) Task Order

Table of Contents

1.0 Introduction

The United States Special Operations Command (USSOCOM) requires comprehensive worldwide information technology (IT) support to operate and maintain the Special Operations Forces (SOF) Information Enterprise (SIE). The SIE is comprised of people, processes, equipment, technology and information that, when utilized together, enable SOF to conduct operations worldwide across Department of Defense (DoD) and other U.S. and foreign government organizational boundaries. The SIE provides support from the garrison level out to forward deployed tactical operators and sensors worldwide. The SIE vision, governance and concept of operations have been documented by the USSOCOM Chief Information Officer (CIO)/J6 in the USSOCOM Information Management directives series and the SIE Operations Order (OPORD). Key elements of the SIE include network operations centers, data centers, enterprise services, and global terrestrial and satellite connectivity. Support for the SIE must be global in extent and address the full spectrum of IT requirements.

USSOCOM, its Component Commands, Theater Special Operations Commands (TSOCs), and deployed forces require IT services that are highly reliable, user friendly, integrated, effective, and easily adapted to ensure mission accomplishment in a dynamic environment. In pursuit of these requirements, USSOCOM, its Component Commands, TSOCs, and deployed forces are deploying the Special Operations Forces Network (SOFNET). With the implementation of

SOFNET, the SIE will have evolved into a true IT enterprise providing features such as single sign-on user accounts, as well as location independent access to enterprise services and portal sites throughout the SIE. SOFNET will extend SIE services throughout USSOCOM's Headquarters (HQ), Component Commands, TSOCs, and deployed forces with corresponding increases in the number of supported locations and the current scale of support.

The deployment of the SOFNET is instrumental to achieving the Commander's Vision of a Global SOF Network that provides strategic options for our national leaders and supported Global Combatant Commanders through a worldwide network that fully integrates our military, interagency and international partners with aligned structures, processes and authorities. The services provided by SITEC II will be a key enabler for over 69,700 users operating in approximately 75 countries.

2.0 Background

USSOCOM was formed in 1987 and is a unified combatant command of the Department of Defense (DoD). USSOCOM's mission is to provide fully capable SOF to defend the United States and its interests and to plan and synchronize operations against terrorist networks. USSOCOM is responsible for training and equipping all DoD SOF to perform missions anywhere in the world at any time. Specific responsibilities of USSOCOM include developing, acquiring, integrating, fielding, and supporting special operations peculiar equipment, material, supplies and systems and ensuring the interoperability of equipment and forces.

USSOCOM is comprised of: a headquarters at MacDill Air Force Base (AFB), FL; one subunified command—the Joint Special Operations Command (JSOC)—at Fort Bragg, NC; and four component commands: the United States Army Special Operations Command (USASOC) at Fort Bragg, NC; the Naval Special Warfare Command (NAVSOC) at Coronado, CA; the Air Force Special Operations Command (AFSOC) at Hurlburt Field, FL; and Marine Corps Forces Special Operations Command (MARSOC) at Camp Lejeune, NC. In addition, each of the Geographic Combatant Commanders has an attached TSOC that provides theater-related special operations strategy and planning efforts.

3.0 Applicable Conditions

The significant conditions that affect the SITEC II acquisition are Locations for Work Performance, Contractor Security, Safeguarding Classified Information Materials, Security Management Support, Compliance with DoD / USSOCOM IT Standards, Security and Classification, Equipment, Compliance with USSOCOM Software Tools, Deployment of Contractors, and other Applicable Conditions. These conditions are further described below.

3.1 Locations and Hours of Work Performance

All support provided by the Contractor under this Task Order shall be performed onsite within facilities provided by USSOCOM, its Component Commands, TSOCs, and deployed forces or other Government provided or designated facilities, unless otherwise agreed upon and approved in advance by the appropriate Government personnel at a given work location (e.g., the associated Contracting Officer's Representative (COR)). The Contractor shall provide global support 24 hours a day, 7 days a week, over the period of performance of the task order unless otherwise stated in this Task Order or approved in advance by the appropriate Government personnel (e.g., associated COR) at the given work location.

3.2 Contractor Security

Security will be in accordance with the attached DD254. The Contractor shall be required to have a Top Secret (TS) facility clearance at the time of proposal submission. The majority of Contractor personnel supporting this Task Order shall require a Top Secret – Sensitive Compartmented Information (TS-SCI) clearance to perform onsite work. After contract award, USSOCOM, its Component Commands, TSOCs, and deployed forces will determine the required security clearance levels that Contractor personnel must hold for performing their specified tasks supporting this Task Order. Hiring of Contractor personnel with the requisite security clearances shall be coordinated with and approved by the COR associated with each work location. At the discretion of the Government, selected individuals supporting this contract will require access to Special Access Program (SAP) information. Access to SAP information requires the requisite security clearance based on a security investigation with a date less than 5 years old and requires employees to undergo additional personnel security screening meeting the DoD SAP directives and policies. The Contractor will require access to TS-SCI, SAP, Communications Security (COMSEC), Alternative Compensatory Control Measures (ACCM), North Atlantic Treaty Organization (NATO) and other designated coalition material in their performance of this effort. Contractors will require access to the Non-Secure Internet Protocol Router Network (NIPRNet), the Secret Internet Protocol Router Network (SIPRNet), the Special Operations Command Research, Analysis, and Threat Evaluation System (SOCRATES) network, and other designated coalition networks and equipment at Government facilities. The Contractor will be authorized to courier classified information up to the TS-SCI level in the performance of official duties upon approval of and designation by the COR associated with their work location.

3.3 Safeguarding Classified Information and Materials

The Contractor shall ensure requirements are fulfilled for: safeguarding classified information and classified materials, obtaining and verifying personnel security clearances, verifying the security clearances and indoctrination of visitors, controlling access to restricted areas, protecting Government property, and the security of automated and non-automated management information systems and data. The Contractor shall prevent unauthorized disclosure of classified and sensitive unclassified information. The Contractor shall immediately notify the Government of any security incident or any indication of a potential unauthorized disclosure or compromise of classified or sensitive unclassified information.

3.4 Security Management Support

The Contractor shall provide security management support. Typical efforts include, but are not limited to, performing classified document control functions, classified materials inventories, program access requests, preparing and monitoring personnel indoctrination and debriefing agreements, and maintaining and using security-related databases.

3.5 Compliance with DoD and USSOCOM IT Standards

The Contractor shall perform system and software design, operations, and maintenance in compliance with applicable Department of Defense (DoD), Defense Intelligence Agency (DIA), Defense Information Systems Agency (DISA), National Security Agency (NSA), United States Cyber Command (USCYBERCOM), USSOCOM, Component Command, TSOC, and deployed forces IT policies, procedures, regulations, directives, standards, guidance, and direction, as well as other applicable documents.

3.6 Security and Classification

The IT infrastructure at USSOCOM, its Component Commands, TSOCs, and deployed forces uses multiple network and computing platforms for processing, storing, routing, and delivery of data, voice, and video communications. The data center server and storage infrastructure supports both non-secure and secure network platforms, including the NIPRNet, SIPRNet, SOCRATES, as well as other designated coalition environments. USSOCOM, its Component Commands, TSOCs, and deployed forces may also use communications platforms not currently identified or defined.

3.7 Equipment

The Government will furnish office space and equipment or access to equipment (i.e., computers, desks, network printers, facsimile machines, copy machines, telephones, etc.) for Contractor personnel performing work in Government facilities under this Task Order.

3.8 Utilizing Software Tools

Due to security requirements, the Contractor must use the suite of office automation, service operations management, and cybersecurity management equipment and software tools provided by the Government for performing day-to-day operations of the SIE while working in either Government or Contractor spaces. The Contractor shall not install or utilize software or hardware that is not authorized for use by USSOCOM, its Component Commands, TSOCs or deployed forces. However, the Contractor is encouraged to recommend the use of new or upgraded software.

3.9 Deployment of Contractors

Travel will be required in support of this effort. All travel shall be approved by the appropriate COR prior to the trip. Contractor staff may be required to travel to locations Outside of the Continental United States (OCONUS), including hazardous duty locations. Such deployments shall be subject to Federal Acquisition Regulation (FAR) 52.228-3, Workers' Compensation Insurance (Defense Base Act). Any such deployment will be authorized by the designated Contracting Officer, unless otherwise delegated.

3.10 Capital Equipment Replacement Program (CERP) and Life Cycle Replacement (LCR) Activities

Timely execution of Government Capital Equipment Replacement Programs (CERPs) and Life Cycle Replacement (LCR) is critical to keeping Government computer and networking assets up-to-date, as well as guaranteeing the utilization of CERP/LCR equipment before it reaches end of life. The type of equipment subject to CERP/LCR includes, but is not limited to, servers, voice, video, and audio hardware, common workgroup devices, end user computing devices and associated peripherals, as well as mobile computing devices. At the beginning of each Government fiscal year, the Contractor shall deliver to USSOCOM, its Component Commands, TSOCs, and deployed forces detailed, achievable, Government-approved plans for performing CERP/LCR actions for the ensuing fiscal year. If the Contractor fails to meet published CERP/LCR targets, the Contractor shall provide a monthly report for how it intends to mitigate CERP/LCR target shortfalls. The Contractor shall maintain custody of CERP/LCR equipment, via hand receipt from the Government, until the Contractor completes associated CERP/LCR actions. During this time, CERP/LCR equipment is "government-furnished property" for repair, maintenance, overhall, or modification as governed by FAR 52.245-1. Contractor CERP/LCR responsibilities include:

- Coordinating and managing accountability of new equipment, replacement equipment, and upgrades. The Contractor shall track the status and location of equipment throughout its life cycle.
- No more than 30 days after the start of the Government fiscal year, providing USSOCOM, its Component Commands, TSOCs, and deployed forces with a yearly plan for upgrading or replacing CERP/LCR equipment in accordance with USSOCOM, Component Command, TSOC, and deployed forces' CERP and LCR policies and procedures.
- Once approved, executing the CERP/LCR plan, and providing a monthly report, delivered no more than five business days after the start of each month, that documents the Contractor's actual CERP/LCR progress against goals in the Contractor's approved plan.
- Providing a plan of action for meeting CERP/LCR goals If the Contractor fails to meet monthly goals.
- Completing LCR/CERP actions no later than 12 months from the receipt of replacement equipment by USSOCOM, its Component Commands, TSOCs, and deployed forces.
- Assuming custody of equipment awaiting installation, equipment awaiting or under repair, and equipment awaiting disposition.
- Processing warranty actions for CERP/LCR equipment, including those items within the Contractor's custody.
- Transporting equipment, including classified equipment, being installed, requiring repair or being processed for disposal.
- Within 45 days of identification, processing end of life, defective, or damaged equipment through Defense Logistics Agency (DLA) Disposition Services (DDS).

3.11 Other Applicable Conditions

Unless stated otherwise in this Task Order or amended by a bilateral modification, the following conditions apply to work performed under this Task Order:

- Align support to USSOCOM, its Components, TSOCs, and deployed forces according to the Tier structure (1-4) outlined in the SIE OPORD.
- Perform preventative maintenance on USSOCOM, Component Command, TSOC, and deployed forces' equipment according to time intervals mandated by the associated Government owner and the manufacturer.
- Only use Government approved and supplied networks, systems and software except with explicit, written permission from the appropriate COR.
- Work in conjunction and collaboration with other Government entities and third party contractors supporting USSOCOM, its Component Commands, TSOCs and deployed forces.
- Provide USSOCOM, its Component Commands, TSOCs, deployed forces and their delegates (including other contractors) free and open access to documents, reports, data, and other artifacts created or modified under this Task Order.
- Assist customers and respond to requests for information in a timely manner..
- Develop and publish best practices, policies, and procedures within the scope of each specified task in accordance with the SIE OPORD.
- Comply with and report any potential violations of the Rules of Behavior to the Government Computer Security Incident Response Team.

- Ensure that Contractor personnel that perform Cybersecurity functions as a part of their assigned duties are compliant with Department of Defense Directive (DoDD) 8140, any subsequent directives provided by DoD, and relevant Service Component instructions or directives. .
- Ensure that relevant Contractor personnel and sub-contractors have proper training on new hardware and software releases prior to the deployment of new hardware and software releases into the IT environment of USSOCOM, its Component Commands, TSOCs, and deployed forces.
- Ensure that Contractor personnel and sub-contractors receive appropriate training on the proper use and configuration of hardware and software utilized by USSOCOM, its Component Commands, TSOCs, and deployed forces, as well as any new or updated hardware and software products purchased by USSOCOM, its Component Commands, TSOCs, and deployed forces over the period of performance of this task order.
- As directed, assist USSOCOM, its Component Commands, TSOCs, and deployed forces with satisfying the requirements of relevant Freedom of Information Act (FOIA) requests, as well as other mandated searches for data and information on the SIE.
- As directed, assist USSOCOM, its Component Commands, TSOCs, and deployed forces with completing activities required to expunge data of a higher classification placed on systems and storage of a lower classification (i.e., “spillages”).
- When required, the Contractor shall perform work on the IT environment in cooperation with military and Government personnel.
- As directed, process end of life, defective, or damaged equipment through DDS.
- As directed, obtain leased vehicles for the transport of hardware and equipment between locations on specified military installations.

4.0 Program Management

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, to satisfy the requirements identified in this Statement of Objectives (SOO). The Contractor shall identify a Program Manager (PM) by name who shall provide management, direction, administration, quality assurance, and leadership for the execution of this Task Order. The identified PM shall serve as the single point of contact for the work performed under this Task Order, including work performed by subcontractors. The PM shall be responsible for issues arising from work across the entire Task Order, as well as the successful resolution of these issues.

The Contractor shall identify a Site Leader by name at the sites identified by USSOCOM, its Component Commands, TSOCs, and deployed forces. The Site Leader shall provide management, direction, administration, quality assurance, and leadership for the execution of this Task Order at their assigned site. Each Site Leader shall serve as the point of contact for work performed under this Task Order at their assigned site, including work performed by subcontractors. The Site Leader shall be responsible for issues arising from work performed under this Task Order at their associated site, as well as the successful resolution of these issues. The Site Leader shall immediately report Task Order related issues to both the associated Government lead and the PM and brief the associated Government lead and PM on the status of these issues until they are resolved.

4.1 Coordinate a Task Order Kick-Off Meeting

The Contractor shall schedule and coordinate a Task Order Kick-Off Meeting at a location approved by the Government. The meeting will provide an introduction between the Contractor personnel and Government personnel involved with the Task Order. The meeting will provide the opportunity to discuss technical, management, and security issues, as well as travel authorization and reporting procedures. At a minimum, the attendees shall include Key Contractor Personnel, the Primary Contracting Officer's Representative (PCOR), and other relevant Government personnel. The Contractor shall provide an updated copy of the Transition Plan (A011) at the Kick-Off meeting.

4.2 Prepare a Contractor Progress, Status and Management Report (CPSMR) (CDRL A003)

The Contractor PM shall develop and provide an CPSMR using Microsoft (MS) Office Suite applications, by the tenth of each month via electronic mail to the PCOR. The CPSMR shall include the following:

- Problems and corrective actions taken. Also include issues or concerns and proposed resolutions to address them. (CDRL A004)
- Personnel gains, losses, and status (e.g., security clearance, etc.).
- Government actions required.
- Summary of trips taken, conferences attended, etc. (attach Trip Reports to the MSR for reporting period).
- Accumulated invoiced cost for each Contract Line Item (CLI) up to the previous month.
- Projected cost of each CLI for the current month.

4.3 Convene Technical Status Meetings

The Contractor PM shall convene a monthly Task Order Activity and Status Meeting with the PCOR and other vital Government stakeholders. The purpose of this meeting is to ensure all stakeholders are informed of the monthly activities and the MSR, to provide opportunities to identify other activities and establish priorities, and to coordinate resolution of identified problems or opportunities. The Contractor PM shall provide minutes of these meetings to the PCOR within five workdays following the meeting. These minutes shall include a list of attendees, issues discussed, decisions made, and action items assigned.

4.4 Prepare a Project Management Plan (PMP) (CDRL A008)

The Contractor shall document all support requirements in a PMP. The PMP shall:

- Describe the proposed management approach.
- Provide for an overall Level 3 Work Breakdown Structure (WBS) and associated responsibilities and partnerships between Government organizations.

The Contractor shall provide the Government with a draft PMP on which the Government will make comments. The final PMP shall incorporate the Government's comments.

The PMP is an evolutionary document that shall be updated annually at a minimum. The Contractor shall work from the latest Government-approved version of the PMP.

4.5 Prepare Trip Reports

The Government will identify the need for a Trip Report when the request for travel is submitted. The Contractor shall keep a summary of all long-distance travel including, but not limited to, the name of the employee, location of travel, duration of trip, and point of contact (POC) at the travel location.

4.6 Staffing Matrix

The Contractor shall develop and update a staffing matrix to show arriving, departing, and transfers of Contractor personnel on the Task Order. The matrix shall include, at a minimum, task numbers, job descriptions, names, arrival and departure dates, and company names.

4.7 Transition-In

The Contractor shall ensure that there will be minimum service disruption to vital Government business and no service degradation during and after transition. The contractor shall conduct a transition in mid point assessment meeting to update the Government on the status of the transition and present the following documents:

- Draft Program Management Plan (CDRL A008)
- Draft Baseline Discription Document (CDRL A001)
- Draft Standard Operating Procidures (CDRL A009)
- Draft Information Security Boundary Configuration Management Plan (CDRL A010)
- Draft Configuration Management Plan (CDRL A002)
- Draft Quality Assurance Program Plan (CDRL A012)

All transition activities shall be completed prior to the end of the transition-in Contract Line Item Nummber (CLIN) period of performance end date and all draft documents shall be finalized and presented to the Government at a Transition-In close out meeting.

4.8 Transition-Out

The Transition-Out Plan shall facilitate the accomplishment of a seamless transition from the incumbent to an incoming contractor or Government personnel at the expiration of the Task Order. The Contractor shall provide and implement a Transition-Out Plan no later than 90 calendar days prior to the expiration of the Task Order. The Contractor shall identify how it will coordinate with the incoming contractor or Government personnel to transfer knowledge regarding the following:

- Project management processes
- Points of contact
- Location of technical and project management documentation
- Status of ongoing technical initiatives
- Appropriate Contractor-to-contractor coordination to ensure a seamless transition
- Transition of Key Personnel
- Actions required of the Government

The Contractor shall also establish and maintain effective communication with the incoming contractor or Government personnel for the period of the transition via weekly status meetings.

5.0 Network Operations (NetOps)

Network Operations (NetOps) encompasses the management and monitoring of systems and networks critical to the Command and Control (C2) of the SOF mission. This is a distributed function federated under the USSOCOM Enterprise Operations Center and supported by Component Network Operations Centers, Theater Network Operations Centers, the Consolidated Service Desk, and local help desks. These organizations, together, provide USSOCOM, it Component Commands, TSOCs, and deployed forces with the necessary situational awareness of the IT infrastructure.

5.1 Network Operations and Monitoring – Enterprise Operations Center (EOC)

The USSOCOM Enterprise Operations Center (EOC) is the Network Operations (NetOps) and network defense element responsible for C2 of the SIE. In this role the EOC monitors and manages the SIE, coordinates planned outages, identifies unplanned outages, tracks planned outages, unplanned outages, and cybersecurity events, reports outages and cybersecurity events, and coordinates and approves network fix actions recommended by the Contractor. The EOC is the NetOps nerve center of the SIE that prioritizes actions while proactively identifying and solving network and security events before they become outages.

The Contractor's duties and responsibilities regarding NetOps and monitoring in the EOC include providing current operations support and subject matter expertise for voice, data, transmission, and video networking, as well as any required coordination between USSOCOM, the United States Cyber Command (USCYBERCOM), USSOCOM's Components and TSOCs, and other subordinate elements. The Contractor shall also maintain situational awareness of the status and performance of USSOCOM's wide area network (WAN), assist with NetOps reporting, help prioritize and synchronize NetOps, and support the implementation of NetOps constructs and policies in accordance with the SIE OPORD. Lastly, the Contractor shall help USSOCOM Components and TSOCs with technical issues related to the operation of the SIE. Specific sub-areas covered in this area include proactive data network monitoring and defense, transmission path monitoring, and Authorized System Interruption (ASI) processing.

The tasks in this area include:

5.1.1 Service Monitoring

- Provide dedicated, on-site Tier 1 and Tier 2 support 24 hours per day, 7 days per week in accordance with the SIE OPORD.

5.1.1.1 Monitor

- Configure Government furnished monitoring tools to provide situational awareness views of USSOCOM networks for higher, peer, and subordinate NetOps Centers, and then maintain these views once configured.
- Utilize Government provided monitoring tools to identify potential incidents or degradations of services, applications, or networks.
- Maintain situational awareness of SIE services, applications, and associated devices.
- Perform proactive monitoring of services and applications for status and health.
- Monitor and evaluate configurations and performance of USSOCOM services.

5.1.1.2 Respond

- Implement network and security access policies.
- Evaluate and respond to event triggers.
- Respond to outages or events via reporting, coordinating changes, applying security patches, coordinating network minimization, and any other relevant actions.
- Respond to requests for technical support from USSOCOM Components, TSOCs, subordinate organizations, and deployed forces.
- Upon discovery of service or application trouble conditions, implement recovery procedures to isolate specific root causes.
- Perform fault and impact analysis on user activity and service performance based on the proactive monitoring of generated network and security faults.
- Troubleshoot and resolve incidents in accordance with the SIE OPORD tier structure and permission groups.
- Escalate incidents to higher tiers within the guidelines of USSOCOM policies, procedures, regulations, and directives.
- Coordinate corrective actions to restore and repair services internally and externally.
- Execute approved changes, responses, and corrective actions where USSOCOM has change authority.
- Coordinate approved changes where outside agencies have change authority.
- Exercise Continuity of Operations (COOP) capability as directed.

5.1.1.3 Analyze

- Create network impact assessments by correlating operational events with the status of systems.
- Analyze the configurations of services and applications in order to correct network anomalies.
- Perform basic analysis of performance and security event trends and identify issues related to associated network devices, connectivity, services, and applications.
- Perform trend analysis and report anomalies

5.1.1.4 Report

- Create incident tickets for event triggers.
- Initiate, update, track, manage, and resolve incident tickets.
- Report impact assessments regarding the status of systems to the Watch Officer and the Operations Officer
- Provide data required to support the development of engineering courses of action (COAs).
- Advise the Watch Officers and the Operations Officer on the capacity and performance of storage, memory, processing, and applications, and recommended courses of action when issues arise.
- Record and archive reports for trend analysis.
- Format and disseminate reports to higher, peer, and subordinate NetOps Centers.
- Generate reports using the USSOCOM ticketing system (primary), email, telephone, web portal posting, message traffic, and database entries.
- Participate in meetings and conferences as directed.

5.1.2 Transmission Path Monitoring

- Provide dedicated, on-site Tier I and Tier 2 support 24 hours per day, 7 days per week in accordance with the SIE OPORD.

5.1.2.1 Monitor

- Configure Government furnished monitoring tools to provide situational awareness views of USSOCOM networks for higher, peer, and subordinate NetOps Centers, and then maintain these views once configured.
- Utilize Government furnished monitoring tools to provide situational awareness views for higher, peer, and subordinate NetOps Centers, and then maintain those views.
- Maintain situational awareness of SIE services and devices.
- Perform proactive monitoring of network elements for status and health.
  a. Monitor and evaluate the configurations and performance of the USSOCOM network.
  b. Monitor logical network topology, including connectivity and routing.
  c. Monitor network device performance.
- Identify transmission network problems and ensure transmission network connectivity is functioning properly.

5.1.2.2 Respond

- Evaluate and respond to event triggers.
- Respond to outages or events via reporting, coordinating changes, applying security patches, coordinating network minimization, and any other relevant actions.
- Respond to requests for technical support from NetOps Centers, Components, TSOCs, subordinate organizations, and deployed forces.
- Upon discovery of network trouble conditions, implement network recovery procedures to isolate specific root causes.
- Perform fault/impact analysis on user activity and network performance based on proactive monitoring of generated network and security faults.
- Troubleshoot and resolve incidents within the SIE OPORD tier structure and permission groups.
- Escalate incidents to higher tiers within the guidelines of USSOCOM policies, procedures, regulations, and directives.
- Coordinate corrective actions to restore and repair network connectivity internally and externally.
- Assist Components, TSOCs, and deployed forces with transmission networks and troubleshooting of issues.
- Coordinate approved changes where outside agencies have change authority.
- Execute approved changes, responses, and corrective actions where USSOCOM has change authority.
- Exercise COOP capability as directed.

5.1.2.3 Analyze

- Create and report impact assessments by correlating operational events with network status.
- Analyze the configurations of network devices and applications to correct network anomalies.
- Perform analysis of performance and security event trends and identify issues related to associated network devices and connectivity.
- Perform trend analysis and report anomalies.

5.1.2.4 Report

- Create incident tickets for event triggers.

- Initiate, update, track, manage, and resolve incident tickets.
- Provide data required to support the development of engineering COAs.
- Report transmission network issues to the Watch Officers and the Operations Officer.
- Generate reports using the USSOCOM ticketing system (primary), email, phone, web portal posting, message traffic, and database entry.
- Record and archive reports for trend analysis.
- Format and disseminate reports to higher, peer, and subordinate NetOps Centers.
- Participate in meetings and conferences as directed.

5.1.3 Authorized System Interruption (ASI) Processing

- Create, manage, track, and coordinate ASIs throughout the SIE in accordance with SIE OPORD.
- Process Component and TSOC ASI requests, tracking ASIs from initial request through completion.
- Process ASIs generated by external Agencies and coordinate them with Components, TSOCs, and other subordinate NetOps Centers.
- Assess the potential impacts of ASIs on network systems, make recommendations to the Watch Officer to assist in the approval process, and, when required, provide technically sound resolutions to Components, TSOCs, and other subordinate NetOps centers that have affected resources.
- Track ASIs using USSOCOM approved systems, provide reports for situational awareness, and brief the status of ASIs to the Watch Officer.
- Maintain required electronic mail distribution lists in order to coordinate ASIs appropriately.
- Maintain the ASI form, as well as any content generated by the form.
- Participate in meetings and briefings as directed.

5.1.4 Incident Management

- Provide dedicated, on-site support 24 hours per day, 7 days per week in accordance with the SIE OPORD.
- Manage the rapid progression of incidents from creation to completion.
- Perform trend analysis on incidents, developing and publishing reports as directed.
- Format and disseminate reports to higher, peer, and subordinate NetOps Centers.
- Participate in meetings and conferences as directed.
- Provide technical analyses of incidents to higher, peer, and subordinate NetOps Centers.
- Document the relationship of incidents to configuration items.

5.1.5 Problem Management

- Identify, track, and interpret trend analyses to create resolutions for potential and ongoing issues.
- As directed, create and implement teams to target or resolve specific problems and facilitate restoration.
- Format and disseminate reports to higher, peer, and subordinate NetOps Centers.
- Participate in meetings and conferences as directed.
- Track and identify incident trends that could be potential problems or have been already identified as a problem.

5.2 Component NetOps Control Center (CNCC)

The Component NetOps Control Centers (CNCCs) are entities that operate 24 hours per day, 7 days per week to provide NetOps and network defense situational awareness to the Component Commanders that operate them, as well as to the USSOCOM EOC. The goal of the CNCCs is to allow Component Commanders to redirect and prioritize the restoration of outages within their logical Area of Responsibility (AOR) and proactively maintain the health and security of the SIE based on mission priority. The CNCCs take direction from their Component Command's leadership and report restoral priorties to the USSOCOM EOC.

The Contractor's duties and responsibilities regarding NetOps and monitoring in the CNCC include providing current operations support and subject matter expertise for voice, data, transmission, and video networking, as well as any required coordination between the Component, USSOCOM, USCYBERCOM, TSOCs, and subordinate elements. The Contractor shall also maintain situational awareness of the status and performance of the Component's WAN, assist with NetOps reporting, and support the implementation of USSOCOM NetOps constructs and policies, including defense of the network. Lastly, the Contractor shall provide technical assistance to subordinate units and TSOCs with issues related to the operation of the SIE. Specific sub-areas covered in this area include data network monitoring and transmission path monitoring.

The tasks in this area include:

5.2.1 Service Monitoring

- Provide dedicated, on-site Tier I and Tier 2 support 24 hours per day, 7 days per week in accordance with the SIE OPORD.

5.2.1.1 Monitor

- Configure Government furnished monitoring tools to provide situational awareness views of the Component Command's logical AOR and unique services, specturms and networks for higher, peer, and subordinate NetOps Centers, and then maintain those views once configured.
- Utilize Government provided monitoring tools to identify potential incidents or degradations of Component Command services, applications, or networks.
- Maintain situational awareness of SIE services, applications, and associated devices within the Component Command's logical AOR.
- Perform proactive monitoring of services and applications for status and health.
- Monitor and evaluate configurations and performance of both USSOCOM and Component Command services.

5.2.1.2 Respond

- Implement network and security access policies.
- Evaluate and respond to event triggers.
- Respond to outages or events via reporting, coordinating changes, applying security patches, coordinating network minimization, and any other relevant actions.
- Respond to requests for technical support from USSOCOM Components, TSOCs, subordinate organizations, and deployed forces.
- Upon discovery of service or application trouble conditions, implement recovery procedures to isolate specific root causes.

- Perform fault and impact analysis on user activity and service performance based on the proactive monitoring of generated network and security faults.
- Troubleshoot and resolve incidents within the SIE OPORD tier structure and permission groups.
- Escalate incidents to higher tiers within the guidelines of both Component Command and USSOCOM policies, procedures, regulations, and directives.
- Coordinate corrective actions to restore and repair services internally and externally.
- Execute approved changes, responses, and corrective actions where the Component Command has change authority.
- Coordinate approved changes where outside agencies have change authority.
- Exercise USSOCOM and Component Command COOP capabilities as directed.

5.2.1.3 Analyze

- Create network impact assessments by correlating operational events with the status of systems.
- Analyze the configurations of services and applications to correct network anomalies.
- Perform basic analysis of performance and security event trends and identify issues related to associated network devices, services, and applications.
- Perform trend analysis and report anomalies.

5.2.1.4 Report

- Create incident tickets for event triggers.
- Initiate, update, track, manage, and resolve incident tickets.
- Report impact assessments regarding the status of systems to the Component Command Watch Officer and Operations Officer
- Provide data required to support the development of engineering courses of action (COAs).
- Advise the Component Command Watch Officers and Operations Officer on the capacity and performance of storage, memory, processing, and applications, and recommended courses of action when issues arise.
- Record and archive reports and store them for trend analysis.
- Format and disseminate reports to higher, peer, and subordinate NetOps Centers.
- Generate reports using the enterprise ticketing system , email, telephone, web portal posting, message traffic, and database entries.
- Participate in meetings and conferences as directed.

5.2.2 Transmission Path Monitoring

- Provide dedicated, on-siteTier 1 and Tier 2 support 24 hours per day, 7 days per week in accordance with the SIE OPORD.

5.2.2.1 Monitor

- Configure Government furnished monitoring tools to provide situational awareness views of the Component Command's networks for higher, peer, and subordinate NetOps Centers, and then maintain these views once configured.
- Utilize Government furnished monitoring tools to provide situational awareness views for higher, peer, and subordinate NetOps Centers, and then maintain those views.
- Maintain situational awareness of services and devices in the Component Command's logical AOR.
- Perform proactive monitoring of network elements for status and health.

  a. Monitor and evaluate the configurations and performance of the network in the Component Command's logical AOR.
  b. Monitor logical network topology, including connectivity and routing.
  c. Monitor network device performance.
- Identify transmission network problems and ensure transmission connectivity is functioning properly.

5.2.2.2 Respond

- Evaluate and respond to event triggers.
- Respond to outages or events via reporting, coordinating changes, applying security patches, coordinating network minimization, and any other relevant actions.
- Respond to requests for technical support from NetOps Centers, Components, TSOCs, subordinate organizations, and deployed forces.
- Upon discovery of network trouble conditions, implement network recovery procedures to isolate specific root causes.
- Perform fault and impact analysis on user activity and network performance based on proactive monitoring of generated network and security faults.
- Troubleshoot and resolve incidents within tier structure and permissions group.
- Escalate incidents to higher tiers within the guidelines of both Component Command and USSOCOM policies, procedures, regulations, and directives.
- Coordinate corrective actions to restore and repair network connectivity internally and externally.
- Assist USSOCOM, other Components, and TSOCs with transmission networks and troubleshooting of issues.
- Coordinate approved changes where outside agencies have change authority.
- Execute approved changes, responses, and corrective actions where the Component Command has change authority.
- Exercise USSOCOM and Component Command COOP capabilities as directed.

5.2.2.3 Analyze

- Create and report impact assessments by correlating operational events with network status.
- Analyze the configurations of network devices and applications to correct network anomalies.
- Perform analysis of performance and security event trends and identify issues related to associated network devices and connectivity.
- Perform trend analysis and report anomalies.

5.2.2.4 Report

- Create incident tickets for event triggers.
- Initiate, update, track, manage, and resolve incident tickets.
- Provide data required to support the development of engineering COAs.
- Report transmission issues to the Component Command's Watch Officers and Operations Officer.
- Generate reports using the enterprise ticketing system (primary), email, telephone, web portal posting, message traffic, and database entries.
- Record and archive reports for trend analysis.
- Format and disseminate reports to higher, peer, and subordinate NetOps Centers.
- Participate in meetings and conferences as directed.

5.3 Theater Special Operations Command (TSOC) NetOps Control Center (TNCC)

The Theater NetOps Control Centers (TNCCs) are entities that operate 24 hours per day, 7 days per week to provide NetOps and network defense situational awareness to the TSOC Commanders that operate them and the USSOCOM EOC. The goal of the TNCCs is to allow TSOC Commanders to redirect and prioritize the restoration of outages and proactively maintain the health and security of the SIE based on mission priority. The TNCCs take direction from their Theater Special Operations Command leadership and report restoral priorties to the USSOCOM EOC.

The Contractor's duties and responsibilities regarding NetOps and monitoring in the TNCC include providing current operations support and subject matter expertise for voice, data, transmission, and video networking, as well as any required coordination between the TSOC, USSOCOM, USCYBERCOM, Components, and subordinate elements. The Contractor shall also maintain situational awareness of the status and performance of The TSOC's WAN, assist with NetOps reporting, and support the implementation of USSOCOM NetOps constructs and policies, including defense of the network. Lastly, the Contractor shall provide technical assistance to subordinate units and their components with issues related to the operation of the SIE. Specific sub-areas covered in this area include data network monitoring and transmission path monitoring.

The tasks in this area include:

5.3.1 Service Monitoring

- Provide dedicated, on-site Tier 1 and 2 support 24 hours per day, 7 days per week in accordance with the SIE OPORD.

5.3.1.1 Monitor

- Configure Government furnished monitoring tools to provide situational awareness views of regional AOR networks for higher, peer, and subordinate NetOps Centers, and then maintain those views once configured.
- Utilize Government provided monitoring tools to identify potential incidents or degradations of services, applications, or networks.
- Maintain situational awareness of SIE services, applications, and associated devices
- Perform proactive monitoring of services and applications for status and health.
- Monitor and evaluate configurations and performance of both TSOC and USSOCOM services in the regional AOR.

5.3.1.2 Respond

- Implement network and security access policies.
- Evaluate and respond to event triggers.
- Respond to outages or events via reporting, coordinating changes, applying security patches, coordinating network minimization, and any other relevant actions.
- Respond to requests for technical support from USSOCOM Components, TSOCs, subordinate organizations, and deployed forces.

- Upon discovery of service or application trouble conditions, implement recovery procedures to isolate specific root causes.
- Perform fault and impact analysis on user activity and service performance based on proactive monitoring of generated network and security faults.
- Troubleshoot and resolve incidents in accordance with the SIE OPORD tier structure and permissions groups.
- Escalate incidents to higher tiers within the guidelines of both TSOC and USSOCOM policies, procedures, regulations, and directives.
- Coordinate corrective actions to restore and repair services internally and externally.
- Execute approved changes, responses, and corrective actions where the TSOC has change authority.
- Coordinate approved changes where outside agencies have change authority.
- Exercise USSOCOM and TSOC COOP capabilities as directed.

5.3.1.3 Analyze

- Create network impact assessments by correlating operational events with the status of systems.
- Analyze the configurations of services and applications to correct network anomalies.
- Perform basic analysis of performance and security event trends and identify issues related to associated network devices, connectivity, services, and applications.
- Perform trend analysis and report anomalies

5.3.1.4 Report

- Create incident tickets for event triggers.
- Initiate, update, track, manage, and resolve incident tickets.
- Report impact assessments regarding the status of systems to the TSOC Watch Officer and Operations Officer
- Provide data required to support the development of engineering courses of action (COAs).
- Advise the TSOC Watch Officers and the Operations Officer on the capacity and performance of storage, memory, processing, and applications, and recommended courses of action when issues arise.
- Record and archive reports for trend analysis.
- Format and disseminate reports to higher, peer, and subordinate NetOps Centers.
- Generate reports using the enterprise ticketing system (primary), email, telephone, web portal posting, message traffic, and database entries.
- Participate in meetings and conferences as directed.

5.3.2 Transmission Path Monitoring

- Provide dedicated, on-site Tier 1 and 2 support 24 hours per day, 7 days per week in accordance with the SIE OPORD.

5.3.2.1 Monitor

- Configure Government furnished monitoring tools to provide situational awareness views of TSOC regional networks for higher, peer, and subordinate NetOps Centers, and then maintain those views once configured.
- Utilize Government furnished monitoring tools to provide situational awareness views for higher, peer, and subordinate NetOps Centers, and then maintain these views.
- Maintain situational awareness of TSOC and SIE services and devices.
- Perform proactive monitoring of network elements for status and health.

    a. Monitor and evaluate the configurations and performance of the TSOC regional AOR network.
    b. Monitor logical network topology, including connectivity and routing.
    c. Monitor network device performance.
- Identify transmission network problems and ensure transmission connectivity is functioning properly.

5.3.2.2 Respond

- Evaluate and respond to event triggers.
- Respond to outages or events via reporting, coordinating changes, applying security patches, coordinating network minimization, and any other relevant actions.
- Respond to requests for technical support from NetOps Centers, Components, TSOCs, subordinate organizations, and deployed forces.
- Upon discovery of network trouble conditions, implement network recovery procedures to isolate specific root causes.
- Perform fault and impact analysis on user activity and network performance based on proactive monitoring of generated network and security faults.
- Troubleshoot and resolve incidents within the SIE OPORD tier structure and permission groups.
- Escalate incidents to higher tiers within the guidelines of both TSOC and USSOCOM policies, procedures, regulations, and directives.
- Coordinate corrective actions to restore and repair network connectivity internally and externally.
- Assist USSOCOM and Components with transmission networks and troubleshooting of issues.
- Coordinate approved changes where outside agencies have change authority.
- Execute approved changes, responses, and corrective actions where the TSOC has change authority.
- Exercise USSOCOM and TSOC COOP capabilities as directed.

5.3.2.3 Analyze

- Create and report impact assessments by correlating operational events with network status.
- Analyze the configurations of network devices and applications to correct network anomalies.
- Perform analysis of performance and security event trends and identify issues related to associated network devices and connectivity.
- Perform trend analysis and report anomalies.

5.3.2.4 Report

- Create incident tickets for event triggers.
- Initiate, update, track, manage, and resolve incident tickets.
- Provide data required to support the development of engineering COAs.
- Report transmission issues to the TOSC Watch Officers and Operations Officer.
- Generate reports using the enterprise ticketing system (primary), email, telephone, web portal posting, message traffic, and database entries.
- Record and archive reports for trend analysis.
- Format and disseminate reports to higher, peer, and subordinate NetOps Centers.
- Participate in meetings and conferences as directed.

5.4 Site/Campus Local Help Desk

The Site/Campus local help desk, if present, is a point of contact for creating, responding to, and resolving end user Incident Reports. It coordinates Incident Reports and Service Request resolution with the proper personnel at the locations that have them,while tracking resolution from initiation to conclusion on behalf of the end user.

The tasks in this area include:

- Ticket creation
- Fixing end user devices
- Basic account maintenance (e.g., password resets, name changes)
- Escalate tickets to the Consolidated Service Desk (CSD) in accordance with the SIE OPORD

5.5 Computer Network Defense (CND)

The Contractor shall perform Computer Network Defense (CND) services, working with system and network administrators, USSOCOM's CND Service Provider (CNDSP), the USSOCOM EOC, and USSOCOM's Component Commands, TSOCs, and deployed forces to protect, monitor, analyze, detect, and respond to cyber incidents on the SIE. The Contractor shall also utilize current intelligence, CND and cybersecurity trends, appropriate situational awareness, and management tools to detect trends, isolate current and future attacks, and identify anomalies or misconfigurations for further investigation at the direction of USSOCOM, its Component Commands, TSOCs, and deployed forces. The Contractor shall maintain situational awareness of CND sensors and tools, notify USSOCOM of sensor and tool outages, and track and report enterprise CND performance and capability metrics in accordance with the SIE OPORD.

5.5.1 Protect, Monitor, Analyze, Detect, and Respond

The Contractor shall perform Computer Network Defense (CND) services, working with system and network administrators, USSOCOM's CND Service Provider (CNDSP), the USSOCOM EOC, and USSOCOM's Component Commands, TSOCs, and deployed forces to employ defensive measures, as well as identify, analyze, and report events that occur or might occur within the network using information collected from a variety of sources in order to protect information, information systems, and networks from threats.

The tasks in this area include:

- Provide dedicated, on-site cyber incident support 24 hours per day, 7 days per week.
- Provide Subject Matter Expertise (SME) to Operational Planning Teams (OPTs) and planning tasks, and assist in the development of CND and Operational Security (OPSEC) measures.
- Maintain, administer, and operate enterprise CND sensors and tools.
- Detect network intrusions and cyber incidents.
- Provide preliminary analysis and identification of cyber incidents.
- Recommend preliminary response actions.
- Perform Tier 2-3 cyber incident analysis to understand the technical details, root causes, and potential impact of incidents.
- Identify and interpret trend analysis reports to isolate nonstandard network traffic
- Perform real-time analysis and event correlation of CND data from enterprise tools.

- Report Commander's Critical Information Requirements (CCIRs), Director's Critical Information Requirements (DCIRs), Priority Intelligence Requirements (PIR), and other information requirements in compliance with USSOCOM, Component Command, TSOC, and USCYBERCOM policies, procedures, regulations and directives, Information Assurance Management (IAM) requirements, and established Standard Operating Procedures (SOPs)/Tactics, Techniques, and Procedures (TTPs).
- Recommend and help direct cyber incident response and recovery
  - Provide containment, risk eradication, recovery, damage assessment and notification recommendations
  - Document the entire cyber incident and related events and activities
- Conduct post-incident analysis and recommend improvements to cyber incident and enterprise policies and procedures.
- Provide expert CND advice and subject matter expertise to USSOCOM, its Component Commands, TSOCs and deployed forces in support of incident handling, course of action development, and related CND response actions.
- Coordinate the integration of CND current operations activities with other NetOps activities at USSOCOM, its Component Commands, TSOCs, deployed forces, and other relevant external agencies.
- Coordinate the integration of CND Watch activities with CND intelligence activities to support intelligence-operations synchronization.
- Recommend changes to policies, procedures, and technologies for improving CND and cybersecurity posture and capabilities.
- Recommend and coordinate network event handling and response actions.
- Assist in the development of CND and Operational Security (OPSEC) reports and data to include:
  - Classified material incidents
  - Joint COMSEC Monitoring Agency reports
  - Information Operations Condition (INFOCON) changes
  - Communication Tasking Order (CTO)/USSOCOM Communications Tasking Order (CTO)/Operational Directive Message (ODM) dissemination, tracking, and compliance monitoring and coordination
  - Daily summary reports of network events and activity relevant to CND practices

5.5.2 CND and Defensive Cyberspace Operations Fusion

The Contractor shall assist in the performance of Computer Network Defense (CND) and Cyberspace operations fusion activities in order to identify complex threats, recommend remediation activities for those threats, as well as develop a fused Defensive Cyberspace Operational picture via the fusion of CND data sources and information from external departments and agencies.

The tasks in this area include:

- Create and deliver daily, weekly, monthly and annual CND activity reports.
- Track and report USSOCOM, Component Command, TSOC, and deployed forces' CND performance and capability metrics.
- Review CND current operations trends to identify anomalies for further investigation.
- At the request of USSOCOM, its Component Commands, TSOCs, and deployed forces, respond to Joint Staff and othertaskers and Requests for Information (RFIs).
- Assist with USSOCOM, Component Command, TSOC, and deployed forces' CND RFI management for both routine and event-related requests.

- Coordinate USSOCOM, Component Command, TSOC, and deployed forces' CND incident record management.
- Maintain and deliver the CND Watch Officers' schedule.
- Examine network topologies to understand data flows through the network.
- Identify and analyze anomalies in network traffic using metadata (e.g., CENTAUR).
- Identify applications and network device operating systems (OSs) based on network traffic.
- Identify network mapping and OS fingerprinting activities.
- Monitor external data sources (e.g., CND vendor sites, Computer Emergency Response Teams, SANS Institute, Security Focus) to maintain situational awareness of CND threat conditions and determine which security issues may have an impact on USSOCOM, its Component Commands, TSOCs, and deployed forces.
- Provide relevant information for threat analysis and response support.
- Coordinate and manage INFOCON changes and track compliance.
- Review current cyber intelligence for relevant threats and develop appropriate actions/response.
- Provide detection, identification, and alerting of possible attacks/intrusions, anomalous activities, and misuse activities, distinguishing these incidents and events from benign activities.
- Receive and analyze network alerts from various sources within the enterprise and determine possible causes of such alerts.
- Reconstruct a malicious attack or activity based on network traffic.
- Triage malware.
- Assist with the distribution of CND intelligence information to the appropriate USSOCOM, Component Command, TSOC, and deployed forces' staff and contractors.

6.0 System and Network Infrastructure

USSOCOM operates a global IT architecture, providing enterprise services defined in the SIE OPORD to its Headquarters, Component Commands, TSOCs, and deployed forces from two interconnected distributed core data centers and multiple Regional Service Centers (RSCs). The Contractor shall operate, maintain, monitor, defend, and manage the hardware, software, and network infrastructure that provide these enterprise services, using subject matter expertise and industry best practices to rapidly and proactively return services to full operation when interruptions occur.

6.1 Network Infrastructure

As a part of managing the enterprise network infrastructure, the Contractor is responsible for engineering, installing, operating, maintaining, monitoring, managing, troubleshooting, improving,and defending the USSOCOM enterprise network infrastructure. This network infrastructure includes multiple, disparate network architectures at various security levels. The Contractor shall support every aspect of network infrastructure management including policies, procedures, implementation, technology integration, and guidance for both scheduled and unscheduled maintenance.

The tasks in this area include:

- Provide support 24 hours a day, 7 days a week for systems, services, and networks operated and maintained as part of the SIE.

- In accordance with the SIE OPORD, the contractor shall establish and manage a comprehensive enterprise network infrastructure maintenance program for enterprise networks, systems, and services. Develop processes and checklists for testing and validating the operational status of enterprise network infrastructure systems and services provided to the enterprise.
- Develop and document an approved enterprise network infrastructure baseline and assist with maintaining configuration control and policy management of devices.
- Maintain enterprise device configurations (to include software) in accordance with cybersecurity Security Technical Information Guides (STIGs) and Communications Tasking Orders (CTOs).
- Develop and document lessons learned during troubleshooting that cover best practices, policies, and procedures on the systems/network environment related to this task.
- Perform trend analysis using historical data collected from the operational network to identify operational issues and areas for improvement. Utilize these trend analyses to recommend network changes and improvements to USSOCOM.
- Manage the USSOCOM enterprise network Internet Protocol (IP) addressing space including unicast and local multicast address assignments for supported networks.
- Manage the USSOCOM, Component Command, TSOC, and deployed forces' Voice and Video dial plan for supported networks.

6.1.1 Network Planning, Design, and Engineering

The Contractor shall provide Tier 4 engineering design and architecture support including engineering support and expertise for voice, video, data, and transmission networks. The Contractor shall develop engineering solutions and COAs to assist with the integration of new technology. The Contractor shall be responsible for Tier 1-3 troubleshooting of enterprise voice, video, and data networks and evaluate the effect of architectural changes on the network.

The tasks in this area include:

- Provide planning and engineering guidance to USSOCOM, Component Command, TSOC, and deployed forces' network planners .
- Assist with network planning for contingencies, exercises, and current and future operations.
- Provide detailed planning of network changes to support emerging requirements.
- Review, edit, publish, and maintain documentation and diagrams of engineering and design activities in agreed upon and accepted industry standard format.
- Identify and recommend tools and processes to accomplish enterprise network operations tasks.
- Provide design and architectural recommendations for long-term/chronic problem resolution.
- Provide Tier –1-3 assistance for immediate and emergency troubleshooting and problem resolution.
- Maintain currency in applicable industry standards from bodies such as the American National Standards Institute (ANSI) and the Institute of Electrical and Electronics Engineers (IEEE), as well as applicable military standards such as Military Construction (MILCON) and Installation Information Infrastructure Architecture (I3A) standards.
- Support the planning, execution, and after-action phases of current operations, contingency operations, and exercises.

- Maintain transmission network diagrams.
- Configure and maintain network management and monitoring tools provided by USSOCOM, its Component Commands, TSOCs, and deployed forces.

6.1.2 Satellite Communications (SATCOM) Planning, Engineering, Operations and Maintenance

USSOCOM utilizes a worldwide satellite communications (SATCOM) network in support of operations at its Headquarters, Component Commands, and TSOCs. Technologies utilized for this network include, but are not limited to, Frequency Division Multiple Accesses (FDMA), Time Division Multiple Access (TDMA), Ultra High Frequency (UHF) Tactical Satellite (TACSAT), INMARSAT Broadband Global Area Network (BGAN), Global Broadcast Satellite (GBS), High-Performance Waveform (HPW), and others. Key areas where USSOCOM requires assistance are operating and maintaining this network, as well as planning, engineering, coordinating, and documenting new connections. Another major task is providing Tier 1-2 support to deployed forces that require help troubleshooting and resolving problems encountered when establishing or maintaining satellite communications.

The tasks in this area include:

- Plan, engineer and operate satellite communications including but not limited to, FDMA, TDMA, UHF TACSAT, GBS, and HPW.
- Provide Tier 1-3 support for satellite communications.
- Provide additional staff as needed to support mission surges and unplanned mission events.
- Create, modify, and update logical satellite circuit connectivity using network monitoring tools provided by USSOCOM, its Component Commands, TSOCs, and deployed forces.
- Provide support for INMARSAT BGAN users.
- Recommend improvements to USSOCOM's satellite communications network and implement those recommendations when approved.
- Process, validate, and determine the impacts of Satellite Access Requests (SAR) and cut sheets for satellite connectivity.
- Provision/allocate resources for validated requirements for SATCOM bandwidth, SATCOM channels, router ports, multiplexer ports, and dedicated circuits.
- Perform circuit engineering to include planning, engineering, and preparing Telecommunications Service Requests/Orders (TSR/TSO).
- Coordinate circuit activation and test with local and remote users including deployed sites.
- Prepare circuit documentation including circuit drawings.
- Provide quality control and bandwidth utilization analyses.

6.1.3 Frequency and Spectrum Management

As a part of planning and executing deployed operations, USSOCOM, its Component Commands, TSOCs, and deployed forces perform Frequency and Spectrum Management in order to avoid radio frequency interference for deployed transmitters and receivers. The Contractor shall provide subject matter expertise with the processes and procedures relative to Frequency and Spectrum Management, including the assignment and management of frequencies for radio networks. The Contractor shall demonstrate expert knowledge of the National Telecommunications and Information Administration (NTIA) Manual of Procedures for Federal Radio Frequency Management.

The tasks in this area include:

- Review frequency assignment proposals to determine whether or not these proposals, if approved, would result in technical conflicts with existing frequency assignments.
- Review frequency assignment proposals for compliance with applicable policy, regulations, and procedures, and recommend corrective action when necessary.
- Understand and use the National Table of Frequency Allocations, various assignment plans, restrictions, rules and procedures for authorizing frequency assignments.
- Perform interference analysis and frequency nomination and processing using Spectrum XXI and the Government Master File (GMF).
- Verify technical equipment specifications to ensure that the data provided in spectrum applications is correct.
- Analyze frequencies already assigned in the proposed operational area for compatibility by considering emission, power, the location of transmitters, the height of antennas, aircraft operation altitude, and other critical equipment operating characteristics.
- Select frequencies and identify alternatives to fulfill new frequency requirements.
- Coordinate frequency related issues with Government and non-Government agencies.
- Prepare applications for Host Nation Coordination utilizing the Host Nation Spectrum Worldwide Database Online (HNSWDO).
- Evaluate and initiate frequency proposals in standard frequency action format in accordance with Military Communications Electronics Board (MCEB) Publication 7.
- Manage line-of-sight (LOS) and beyond line-of-sight (BLOS) voice and data radio networks.
- Perform site surveys and assist in the development of communications plans.
- Prepare and review applicable Spectrum Management documentation.

6.1.4 Wide Area Network/Metropolitan Area Network (WAN/MAN)

USSOCOM operates and maintains Wide Area Network (WAN) and Metropolitan Area Network (MAN) infrastructures at various security classifications around the world. The Contractor shall provide full lifecycle support of USSOCOM's WAN and MAN infrastructure. The Contractor shall provide network installation, tuning, testing, monitoring, upgrading, patching, break/fix, defense, and management of USSOCOM WAN and MAN routing and switching infrastructures, including network hardware and software. The Contractor shall follow USSOCOM-designated network standards for the design, installation, and maintenance of USSOCOM WAN and MAN infrastructures.

The tasks in this area include:

- Plan, design, engineer, configure, install, operate, maintain, troubleshoot, and repair USSOCOM WAN/MAN capabilities, including point-to-point circuits, satellite connectivity, dedicated Internet connections, broadband Internet connections (e.g., digital subscriber line (DSL), cable modem), and Internet based virtual private networks (VPNs).
- Plan, design, engineer, configure, operate, maintain, troubleshoot, and repair USSOCOM WAN/MAN infrastructures, to include necessary additions and changes to associated routers, switches, external USSOCOM and commercial provider circuits and encryption devices.

- Plan, design, engineer, configure, operate, maintain, troubleshoot, and repair USSOCOM WAN/MAN Programs of Record (PORs) (e.g., SDN-L/M/H, SCAMPI, SOFTACS).
- Implement network and security access policy.
- Provision, operate, manage, and monitor USSOCOM WAN/MAN VPN services to securely connect remote USSOCOM elements and mission partners over the SIE and shared public IP networks while ensuring compliance with applicable DoD, DIA, DISA, USCYBERCOM, and USSOCOM policies, procedures, regulations, and directives.
- The Contractor shall be responsible for Tier 1-3 troubleshooting of USSOCOM enterprise WAN/MAN voice, data, and transmission networks and evaluate the effect of architectural changes on the network.
- Configure, update, monitor, manage, troubleshoot and document routers and switches in the USSOCOM WAN/MAN networks.
- Participate in and support USSOCOM, Component Command, TSOC, and deployed forces' exercises (e.g., COOP exercises and events, network vulnerability, "red team/blue team" activities, etc.).
- Collaborate and coordinate with external Government and commercial circuit providers to expedite the restoration of circuit outages.
- Maintain COMSEC cleared personnel with COMSEC courier authorization.

6.1.5 Campus Area and Local Area Network (CAN/LAN)

USSOCOM, its Component Commands, TSOCs and deployed forces operate and maintain Campus Area Network (CAN) and Local Area Network (LAN) infrastructures at various security classifications around the world. The Contractor shall provide full lifecycle support of these CAN and LAN infrastructures. The Contractor shall provide installation, tuning, testing, operating, monitoring, upgrading, patching, break/fix, defense and management of CAN and LAN routing and switching infrastructure hardware and software. The Contractor shall follow USSOCOM-designated network standards for the design, installation, and maintenance of CAN and LAN infrastructures.

The tasks in this area include:

- Plan, design, engineer, configure, operate, maintain, defend, troubleshoot, and repair USSOCOM, Component Command, TSOC, and deployed forces' CAN/LAN capabilities, including point-to-point circuits, dedicated Internet connections, and broadband Internet connections (e.g., DSL, cable modem) to include necessary additions and changes to associated routers, switches, and encryption devices.
- Plan, design, engineer, configure, operate, maintain, defend, troubleshoot, and repair USSOCOM, Component Command, TSOC, and deployed forces' CAN/LAN Programs of Record (PORs) (e.g., C4IAS, SDN, TACLAN).
- Plan, design, engineer, configure, maintain, defend, troubleshoot, and repair the Virtual Local Area Network (VLAN) architectures of USSOCOM, its Component Commands, TSOCs, and deployed forces.
- Plan, design, engineer, configure, maintain, defend, troubleshoot, and repair USSOCOM, Component Command, TSOC, and deployed forces' classified and unclassified wireless LANs (e.g., WiFi), including wireless access points and their interconnection to the wired infrastructure.
- Provision, operate, manage, and monitor USSOCOM VPN services to securely connect remote USSOCOM elements and mission partners over the SIE and shared public IP

networks while ensuring compliance with applicable DoD, DIA, DISA, USCYBERCOM, and USSOCOM policies, procedures, regulations, and directives.

- The Contractor shall be responsible for Tier 1-3 troubleshooting of USSOCOM, Component Command, TSOC, and deployed forces' CAN/LAN voice and data networks and evaluate the effect of architectural changes on them.
- Configure, update, monitor, manage, troubleshoot and document routers and switches in USSOCOM, Component Command, TSOC, and deployed forces' CAN/LAN networks.
- Participate in and support USSOCOM, Component Command, TSOC, and deployed forces' exercises (e.g., COOP exercises and events, network vulnerability, "red team/blue team" activities, etc.).
- Maintain COMSEC cleared personnel with COMSEC courier authorization.

6.1.6 Cable Plant

The Contractor shall engineer, install, test and maintain the secure/non-secure voice, video, data, and radio frequency cable infrastructure at USSOCOM, its Component Commands, TSOCs, and deployed forces. The Contractor shall perform its work in accordance with USSOCOM, Component Command, TSOC and deployed forces' policies, procedures, regulations and directives, as well as the National Electric Contractors Association (NECA)/Building Industry Consulting Service International (BICSI) 568 standard which defines minimum requirements and procedures for installing telecommunications cable infrastructure. This standard also describes professional workmanship.

The tasks in this area include:

- Provide dedicated, on-site coverage for cabling maintained by USSOCOM, its Component Commands, TSOCs, and deployed forces. On-call support shall be provided during non-duty hours. The maximum time for reporting to duty station after on-call support is requested is one hour from the time of notification. The Contractor shall maintain a comprehensive on-call/alert roster and update this roster on a monthly basis.
- Install, replace, repair, remove, terminate, and test new and existing LAN cabling, to include copper (both shielded and unshielded), fiber optic (both single mode and multi-mode), Radio Frequency (RF), specialized cable, e.g. Cable TV, Plain Old Telephone System (POTS), Integrated Services Digital Network (ISDN), and Audio and Video (AV) in accordance with applicable DoD, DIA, DISA, USSOCOM, Component Command, TSOC, and deployed forces' policies and industry best practices.
- Maintain cable infrastructure labeling standards IAW USSOCOM, Component Command, TSOC, and deployed forces' policies, procedures, regulations and directives.

6.2 Unified Capabilities (UC)

USSOCOM, its Component Commands, TSOCs, and deployed forces use converged voice, video, and data communications around a common Internet Protocol (IP)-based infrastructure, which simplifies making telephone calls, sending messages, and joining audio or video conferences. As a growing force multiplier, these Unified Communications (UC) continue to enhance the mission of USSOCOM, its Component Commands, TSOCs, and deployed forces as a source of both wide area collaboration and long distance situational awareness. The proper distribution and handling of UC technologies requires a staff knowledgeable in existing solutions, as well as emerging standards. The Contractor shall support UC services, including planning, designing, engineering, operating, maintaining, defending, and properly employing UC at USSOCOM, its Component Commands, TSOCs, and deployed forces.

6.2.1 Voice and Video Over Internet Protocol (VVoIP)

USSOCOM, its Component Commands, TSOCs, and deployed forces operate multiple Voice and Video over Internet Protocol (VVoIP) Cisco Unified Communications Managers (CUCM), Video Communications Servers (VCS), Unified Contact Center Express (UCCX) software, associated physical and virtual servers, and other call control infrastructure devices that provide video and voice services over a data network. USSOCOM, its Component Commands, TSOCs, and deployed forces operate call control devices on several disparate networks at various levels of classification at sites around the world. The Contractor shall operate, maintain and defend call control infrastructures in accordance with the SIE OPORD, as well as plan, engineer, coordinate, document, and execute changes, upgrades, or installations authorized by USSOCOM, its Component Commands, TSOCs, and deployed forces. The Contractor shall manage and monitor the operation of call control devices to ensure their proper operation and proactively troubleshoot, analyze, and isolate the root cause of issues when they arise. The Contractor shall recommend courses of action to return affected systems to full operational status.

The tasks under this area include:

- Provide dedicated, on-site support 24 hours a day, 7 days a week, 365 days a year.
- Operate, maintain, defend, administer, manage, and provision CUCM's, VCS, UCCX at USSOCOM, its Component Commands, TSOCs, and deployed forces, including required coordination with posts, camps, stations and other service providers
- Proactively monitor the health and performance of VVoIP infrastructures.
- Engineer, coordinate, and document changes, upgrades, or installations authorized by USSOCOM, its Component Commands, TSOCs and deployed forces.
- Troubleshoot, analyze, isolate, and document the root cause of VVoIP issues when they arise.
- Recommend courses of action to correct VVoIP issues and then implement those selected by USSOCOM, its Component Commands, TSOCs and deployed forces.
- Perform dial plan administration.
- Provide VVoIP device feature administration.
- Configure VVoIP directory services.
- Configure interfaces to external voice and video-processing applications.
- Employ applications such as IVR and call attendant consoles.
- Recommend upgrades to VVoIP infrastructures at least annually and incorporate approved upgrades when acquired by the Government.

6.2.2 Video Teleconferencing (VTC) Multipoint Conference Units (MCUs)

USSOCOM, its Component Commands, TSOCs, and deployed forces provide VTC Multipoint Conference Unit (MCU) bridged services for their users on several disparate networks at various levels of classification. The Contractor shall operate, maintain, and defend MCUs in accordance with the SIE OPORD, as well as plan, engineer, coordinate, document, and execute changes, upgrades, or installations authorized by USSOCOM, its Component Commands, TSOCs, and deployed forces. The Contractor shall proactively monitor the operation of MCU VTC sessions on behalf of end users to ensure their proper operation. The Contractor shall troubleshoot, analyze, and isolate the root cause of issues that arise during a live VTC. The Contractor shall then recommend courses of action to return affected systems to full operational status.

The tasks in this area include:

- Provide dedicated, on-site support 24 hours a day, 7 days a week, 365 days a year.

- Install, configure, integrate, test, maintain, operate, and defend teleconferencing hardware and software including MCU VTC bridges and ISDN VTC gateways.
- Plan, install, configure, operate, maintain, defend, manage, repair, and update the Cisco TelePresence Management Suite (TMS), to include performing software updates, account management, and conference scheduling.
- Provide version control and provisioning for VTC coder/decoders (CODECs).
- Establish VTC connectivity to other locations and equipment.
- Schedule, coordinate, and administer multiple simultaneous VTC sessions.
- Recommend upgrades to VTC systems at least annually and incorporate approved upgrades when acquired by the Government.
- Manage, maintain, and post a daily MSL and shift change procedures to ensure proper information flow across shifts. This MSL shall provide a record of maintenance requirements, functions, and corrective actions taken. The Contractor shall document when the deficient function or operation was first discovered/reported, as well as the exact time it was corrected, and when the service, function or operation was restored.
- Proactively monitor VTC services to facilitate the early detection of incidents, impending outages or degradations.
- Schedule, configure, and connect users to Global Video Services (GVS) and Defense Information Systems Network (DISN) Video Services (DVS) conferences.
- Schedule, configure, and connect users to Joint Worldwide Intelligence Communications System (JWICS) VTC conferences.
- Maintain DISA GVS and JWICS VTC gateways.
- Provide remote Tier 2-3 support for deployed VTC endpoints.
- Train USSOCOM, Component Command, TSOC, deployed forces', and other Contractors on the operation of VTC equipment.

6.2.3 Streaming Video/Full Motion Video

USSOCOM, its Component Commands, TSOCs, and deployed forces distribute video across their campuses utilizing various methods and technologies. This includes dissemination and broadcast of television stations and full motion video from both live sources and stored files.

The tasks in this area include:

- Support the distribution of television over IP within USSOCOM, Component Command, TSOC, and deployed forces' facilities. USSOCOM, its Component Commands, TSOCs and deployed forces will determine the number of sources and channels to distribute.
- Support set top boxes, video servers, High Definition (HD) audio/video (A/V encoders and decoders, and program content from non-terrestrial sources.
- Support distribution of full motion video imagery from terrestrial and non-terrestrial sensors and storage.
- Plan, install, configure, operate, maintain, defend, manage, and repair streaming media distribution servers and software (e.g., VBrick, VBrick Enterprise Media System (VEMS), VBrick Distributed Media Engines, Microsoft Windows Media Server, etc.).
- Install, configure, integrate, operate, manage, repair, and update new and existing streaming video sources.

6.3 Message Center

The contractor shall operate Message Centers for USSOCOM, its Component Commands, TSOCs, and deployed forces. This consists of managing C2 systems such as the Automated Message Handling System (AMHS) and the Top Secret Collateral (TS/C) Decision Agent Client. The Contractor shall provide support to USSOCOM, its Component Commands, TSOCs, and deployed forces by managing their Organizational Message System (OMS) directory entries.

The tasks in this area include:

- Operate and manage garrison Organizational Messaging Systems. This includes, but is not limited to, hardware and software for the AMHS Servers.
- Coordinate software maintenance to include troubleshooting, testing, and applying Field Engineering Notes (FENs), software updates and cybersecurity updates in accordance with OMS Program Management Office direction.
- Monitor and respond to service messages, directory scan reports, and DISA Interim Procedures.
- Provide OMS software and hardware configuration control and licensing accountability by developing and maintaining an OMS software and hardware configuration control and licensing repository.
- Provide notification and routing based on message precedence for hardcopy Special Category (SPECAT) and Top Secret message traffic to appropriate organizations in accordance with USSOCOM, Component Command, TSOC, and deployed forces' policies, procedures, regulations, and directives. This includes telephone notification, electronic mail, logging, and receipt.
- Maintain complete chain of custody logs for SPECAT messages.
- Prepare for Organizational Messaging System (OMS) Program Management Office (PMO) inspections and NSA audits.
- Prepare unclassified and classified message systems for deployments.
- Maintain OMS detailed designs for normal operations, as well as in support of exercises and real world contingencies.
- Notify USSOCOM, its Component Commands, TSOCs, and deployed forces of proposed and approved OMS PMO baseline changes as they relate to organizations operating OMS systems.
- Manage OMS directory entries on behalf of USSOCOM, its Component Commands, TSOCs, and deployed forces.

6.4 System Infrastructure

USSOCOM, its Component Commands, TSOCs and deployed forces own system infrastructures utilizing a number of core IT technologies, such as servers, storage, databases, and web/portal servers. These system infrastructures, in turn, provide individual services, which are typically an interconnected set of technologies that rely on each other to provide an intended functionality. The sections below outline the Contractor's responsibilities with regard to installing, configuring, operating, maintaining, defending, troubleshooting, and repairing the equipment in each of these technology areas for USSOCOM, its Component Commands, TSOCs, and deployed forces.

6.4.1 Servers

USSOCOM, its Component Commands, TSOCs, and deployed forces operate data centers with associated physical and virtual server infrastructure at sites across the world. The Contractor shall operate, maintain, and defend this server infrastructure in accordance with USSOCOM, Component Command, TSOC, and deployed forces' policies, procedures, regulations, and directives, as well as plan, engineer, improve, coordinate, document, and execute any changes, upgrades, or installs authorized by USSOCOM, its Component Commands, TSOCs and deployed forces. The Contractor shall also proactively manage and monitor the operation of physical and virtual servers to ensure their proper operation and troubleshoot, analyze, isolate and document the root cause of issues when they arise. As required the Contractor shall then recommend courses of action for returning affected systems to full, operational status within timelines specified by USSOCOM, Component Command, TSOC, and deployed forces' policies and procedures.

The tasks in this area include:

- Provide dedicated on-site support 24 hours a day, 7 days a week, 365 days a year.
- Provide robust and secure day-to-day operations by maintaining, managing, monitoring, and administering server systems on USSOCOM, Component Command, TSOC, and deployed forces' networks.
- Maintain and administer hardware, software, firmware, and operating systems for USSOCOM, Component Command, TSOC, and deployed forces' servers.
- Advise USSOCOM, its Component Commands, TSOCs, and deployed forces regarding required modifications or upgrades, including vendor recommended patches and updates, to servers, software, and services.
- Provide USSOCOM, its Component Commands, TSOCs and deployed forces with a Plan of Action and Milestones (POAM) for recommended modifications and upgrades to servers, software, and services.
- Monitor servers, applications and services using approved monitoring software to facilitate proactive response to hardware failure, misconfiguration, lack of capacity, over subscription, excessive latency, service degradation, and outages.
- Provide server cybersecurity (e.g., Information Assurance Vulnerability Alert (IAVA) assessment compliance, Vulnerability Management System (VMS) reporting, STIG compliance, status of vendor security updates), health (e.g., disk and central processing unit (CPU) utilization) and status reports.
- Configure, manage, and maintain the physical and virtual computing infrastructure associated with services on networks and systems in accordance with the SIE OPORD.
- Provide USSOCOM, its Component Commands, TSOCs, and deployed forces with Subject Matter Expertise on server operations and maintenance.
- Produce an initial written report per the SIE OPORD after an unplanned outage that contains the reason for the outage (i.e., root cause analysis) and technically viable and acceptable courses of action for repair.
- Provide, maintain, and update the following documentation at a minimum:
  - Inventory and status of assets and spare equipment
  - Government approved Prioritized Service Restoration List
  - Physical and Logical Diagrams of systems and their associated storage
  - Operational Checklists documenting standard TTPs for executing tasks required to support server operations and services
  - Consolidated folder of best practices, policies and procedures.
  - Server Security Report (including IAVA compliance status, VMS reporting, STIG compliance, status of vendor security updates, etc.)
  - Server Health Report
  - Rack elevation diagrams
  - SOPs

6.4.1.1 Services

A robust services support program ensures that key and supporting services are reliable and available to end users when needed. As such, the Contractor shall establish and operate a services support program that provides systems administration, maintenance, computer security, and support for servers on USSOCOM networks in accordance with the SIE OPORD. The Contractor shall also operate and maintain items such as servers (physical and virtual), firmware, operating systems, and software. The Contractor shall ensure that services are accessible through the creation and maintenance of user accounts, profiles, print and disk services, data file services, Domain Name Services, and other means.

The Contractor shall have Tier 1-3 expertise in the following areas:

- Messaging with expertise in electronic mail, chat, and video teleconferencing
- Database management.
- Thin Client technology and Virtual Desktop Infrastructure
- Directory Services/Domain Name Service (DNS)
- Dynamic Host Configuration Protocol (DHCP) services for supported networks.
- Storage with expertise in Storage Area Networks (SAN), Network Attached Storage (NAS), Internet Small Computer Systems Interface (iSCSI), and Direct Attached Storage (DAS) technologies
- Portal/Web development with expertise in the design of medium to large Microsoft SharePoint farms (SharePoint 2010 and above), geographical replication, interfacing with external data sources, and integration of third party add-ons
- Public Key Infrastructure (PKI)/Certificate Authority Services
- Customer Relationship Management (CRM)
- Disaster Recovery/Backup and Restore
- Server Virtualization.
- Automatic failover and COOP technologies for services.
- Risks and risk mitigation strategies related to cybersecurity and CND in accordance with applicable DoD and Intelligence Community (IC) directives

6.4.2 Storage Management

The USSOCOM enterprise contains various types of tiered data storage resources in support of enterprise operations. These resources include SAN arrays, NAS, RAID arrays, iSCSI arrays, storage virtualization, and archival/tape backup solutions. The Contractor shall operate, maintain, and defend these storage resources in order to meet the operational needs of the USSOCOM, its Component Commands, TSOCs, and deployed forces.

The tasks in this area include:

- Provide dedicated on-site support.
- Configure, allocate, provision, and manage storage resources located in the USSOCOM.
- Perform capacity planning for storage resources.
- Maintain hardware and software systems and tools used to monitor, maintain, tune, and report on storage environment health and status.
- Advise USSOCOM, its Component Commands, TSOCs, and deployed forces regarding any required modifications or upgrades to storage equipment and software, including

any vendor recommended patches and updates.Provide USSOCOM, its Component Commands, TSOCs and deployed forces with a Plan of Action and Milestones (POAM) for recommended modifications and upgrades to storage equipment and software.

- Monitor and manage storage system tiers and perform onsite "Break/Fix" support for storage resources located within USSOCOM, its Component Commands, TSOCs, and deployed forces in response to incidents, reconfigurations, installations, or other physical changes.
- Remove data accidentally migrated from higher classification systems to lower classification systems (i.e., "spillages") from both online storage and archived backup media.

6.4.3 Global Command and Control System (GCCS)

The Contractor shall be responsible for ensuring system availability and reliability of the Global Command and Control System - Joint (GCCS-J) and related GCCS Family of Systems (FoS) on the networks . The Contractor shall provide technical support to USSOCOM, its Component Commands, TSOCs, and deployed forces. The Contractor shall implement GCCS program requirements. The Contractor shall be responsible for maintenance, troubleshooting, installation, configuration, and the implementation of existing and future versions of the GCCS FoS.

The Contractor shall provide system administration support, technical support, and subject matter expertise for GCCS FoS, including:

- Common Operational Picture (COP)
- Integrated Imagery and Intelligence (I3)
- Joint Operation Planning and Execution System (JOPES)
- Agile Client (AC)
- Joint Command and Control User Interface (JC2CUI)
- Cybersecurity and Client/Server installation
- Theater Air Missile Defense (TAMD) and various GCCS-J subsystems

The tasks in this area include:

- Provide management, system administration, planning, and operational support for C2 servers and client assets, including Microsoft Windows, UNIX/Solaris, Linux/Red Hat systems, within the scope of this task.
- Administer and provide technical support for GCCS FoS assets employed at USSOCOM, its Component Commands, TSOCs, and approved global locations.
- Perform Project Management including Configuration Management.
- Ensure cybersecurity compliance for GCCS FoS assets.
- Perform any necessary actions required to respond to GCCS FoS problem reports.
- Perform system, security, and operational testing/evaluation events.
- Provide support for fielding of future releases.
- Ensure USSOCOM, Component Command, TSOC, and deployed forces' personnel and Contractors are trained on the GCCS FoS systems and maintain an ongoing training program.
- Manage and administer the Radiant Mercury Cross Domain Solution (CDS) or other designated CDS in support of the GCCS mission.

- Plan, design, and implement system backup and recovery operations on GCCS FoS assets.
- Provide management, system administration, planning, and operational support for C2 client assets, including Microsoft Windows systems.
- Administer GCCS FoS client assets employed at USSOCOM, its Component Commands, TSOCs, and deployed forces.

6.4.4 Database Administration

USSOCOM, its Component Commands, TSOCs, and deployed forces operate and maintain various commercial software database systems as supporting software for their services. The Contractor shall plan, engineer, install, configure, maintain, operate, defend, troubleshoot, and repair database systems and servers. The Contractor shall serve as a subject matter expert on these database systems and their integration with other software systems.

The tasks in this area include:

- Provide dedicated on-site support.
- Operate, maintain, and administer database hardware and software in support of USSOCOM, its Component Commands, TSOCs, and deployed forces.
- Provide technical problem solving for customer support of database applications.
- Develop, implement, and maintain Microsoft Structured Query Language (SQL), MySQL, Oracle, UNIX-based, and Linux-based databases.
- Support the implementation of databases using SQL, Active Server Pages (ASPs), .NET, Visual Basic (VB), and Javascript.
- Troubleshoot issues with existing or developed database systems; work with the appropriate personnel to resolve them.
- Write Stored Procedures and Triggers as needed in database development.
- Develop and document system administration, database management, and user guidance.
- Provide input to database policy guidance to USSOCOM, its Component Commands, TSOCs, and deployed forces, and, upon approval, implement necessary changes.

6.4.5 Web/Portal Administration

USSOCOM, its Component Commands, TSOCs, and deployed forces operate and maintain a mixture of both traditional web servers and Microsoft SharePoint infrastructure. The Contractor shall plan, engineer, install, configure, maintain, operate, defend, troubleshoot, and repair web/portal servers. This includes support for the underlying web/portal server technology. The Contractor shall also develop and integrate new content, code, and data sources.

The tasks in this area include:

- Provide dedicated on-site support.
- Plan, engineer, install, configure, maintain, operate, defend, troubleshoot, and repair web/portal servers.
- Administer, manage, configure, and install multiple, disparate Microsoft SharePoint environments.
- Administer, manage, configure, and install multiple, disparate HyperText Markup Language (HTML)-based web sites.
- Develop and document web site architectures and best practices.

- Maintain currency on the following technologies used for the operations and maintenance of web servers: SQL, ASP, .NET, VB, HTML5, and Javascript.
- Develop database interfaces to web servers.

6.4.6 Public Key Infrastructure (PKI)

The Contractor shall operate a Public Key Infrastructure (PKI) and associated help desk to support USSOCOM, Component Command, TSOC, and deployed forces' users. The primarily focus of this effort is to support existing users with certificates/tokens, to issue certificates/tokens to new personnel, and to assist with the development and drafting of PKI policies and procedures.. The Contractor shall ensure compliance with published Department of Defense (DoD) PKI directives.

The tasks in this area include:

- Issue, troubleshoot, and replace SIPR tokens.
- Plan, engineer, install, configure, maintain, operate, defend, troubleshoot, and repair local registration authority tools and systems.
- Plan, engineer, install, configure, maintain, operate, defend, troubleshoot, and repair online certificate status protocol architectures and certificate revocation lists.
- Submit to DISA, as necessary, requests for certificate issuance and track and maintain the validity and revocation of server based certificates.
- Recommend, and upon approval, maintain policies and procedures for USSOCOM, Component Command, TSOC, and deployed forces' PKI programs.
- Reset user Personal Identification Numbers (PINs) and update e-mail addresses on DoD Common Access Cards (CACs) when requested.

6.5 Deployed Systems Support

In addition to its garrison systems, USSOCOM, its Component Commands, and TSOCs also deploy systems and networks in support of exercises and contingencies, both within the Continental United States (CONUS) and OCONUS. The Contractor shall provide system and network technicians with the necessary skillsets to install, uninstall, configure, operate, maintain, defend, update, diagnose, troubleshoot and repair deployed systems and networks. The Contractor shall provide subject matter experts for deployed systems and networks and train deploying and deployed personnel during exercises, in formal schools, and during real world operations. .

7.0 End User and Common Device Support

USSOCOM, its Component Commands, TSOCs, and deployed forces require the services of a highly qualified service provider with the skills and experience to provide support for provisioning, operating, defending, administering, troubleshooting, repairing, and managing end user computing, common area IT, and mobile computing devices. The end user computing environment includes desktop/tower computers, laptop computers, thin client terminals, mobile computing devices, tablets, associated peripheral devices and locally-attached printers, network-attached printers, scanning devices, copiers, digital senders, multi-function devices, plotters, facsimile machines, non-secure and secure desktop telephone equipment, computer kiosks, whiteboards/smartboards, conference room and desktop VTCs and associated A/V devices, conference room phone devices, hallway video displays, digital signage, smart boards, and multi-display clocks. It includes associated operating system software, office productivity software, desktop/laptop image management equipment and software, diagnostics and testing tools, repair tools, remote control take-over capability, automated software update tools, hardware and software tools used to manage end user computing resources, and any other technology that may be deployed in the future to meet USSOCOM's end user computing objectives.

The Contractor shall provide operations and maintenance support for client computing devices, including thick clients, thin clients, laptops, wireless devices and peripherals located at USSOCOM, its Component Commands, TSOCs, and deployed forces locations around the world. For computer systems, peripherals, and other hardware devices, the Contractor shall establish a technical support program to install, maintain, upgrade, replace, and, in the event of a failure or degradation in performance, analyze, troubleshoot, and restore systems/devices to operational status. The Contractor shall plan, engineer, coordinate and manage equipment installations.

7.1 Desktop Computing Devices

USSOCOM, its Component Commands, TSOCs, and deployed forces provide their users desktop computing devices to allow users to perform their day-to-day duties. These devices include virtual desktop infrastructure (VDI) clients, thick clients, laptops, and tablets. Along with these devices users may also have a monitor, keyboard, mouse, Common Access Card (CAC) reader, non-secure telephone, Secret Voice over Internet Protocol (SVoIP) telephone, Keyboard-Video-Mouse (KVM) switch, A/B switch, web camera, microphone, speakers, Compact Disc (CD) burner, desktop VTC, direct attached printer, and other types of directly attached peripheral devices USSOCOM may approve for installation.

7.1.1 Virtual Desktop Infrastructure (VDI) Client

The Contractor shall manage and provide day-to-day support for VDI clients. A VDI client is defined as an end user device with computing capability limited to providing a graphical user interface (GUI) to display and manipulate user data, provide access to user applications, and manage network connectivity and input/output communications processing with a server; the server runs all applications, performs all data processing, manages all security, and handles storage and retrieval of end user data. A VDI client has access to a server which runs a copy of the USSOCOM standard software "core" image along with any other authorized software.

The tasks in this area include:

- Recommend upgrades to and replacements for hardware and software utilized by VDI clients in accordance with the SIE OPORD.
- Integrate, test, and verify VDI client hardware and software with USSOCOM's VDI client "core" image.

7.1.2 Thick Client

The Contractor shall manage and provide day-to-day support for Thick Client workstations. A Thick Client Seat is defined as an end user device with computing and storage capability to provide the end user GUI, to locally install and run end user applications, to directly perform data processing and manipulation, and to store and retrieve end user data from locally-installed/attached data storage devices. A Thick Client Seat provides access and connectivity to computing resources on one of various network enclaves. A Thick Client device runs a copy of the USSOCOM standard software "core" image along with any other authorized software

The tasks in this area include:

- Recommend upgrades to and replacements for hardware and software utilized by thick clients in accordance with the SIE OPORD.
- Integrate, test, and verify VDI client hardware and software with USSOCOM's VDI client "core" image.

7.1.3 Laptops and Tablets

The Contractor shall manage and provide day-to-day support for Laptops and Tablets that provide local or remote access to USSOCOM, its Component Commands, TSOCs, and deployed forces, whether using wired or wireless connectivity. A Laptop/Tablet Seat is a portable, stand-alone type of Thick Client that performs office automation functions, either from the user's normal duty location or from remote locations. Due to their special configuration and purpose, Laptops and Tablets require their own customized version of the USSOCOM software "core" image and authorized software.

The tasks in this area include:

- Recommend upgrades to and replacements for remote access solutions hardware and software utilized by Laptops and Tablets, including any associated wireless and cellular technology in accordance with the SIE OPORD and policies, procedures, ect..
- Integrate, test and verify remote access hardware and software with USSOCOM's Laptop and Tablet images.

7.1.4 Desktop VTC Equipment

USSOCOM provides some personnel with desktop VTC equipment for secure and non-secure communication with personnel both inside and outside of USSOCOM. The Contractor shall manage and provide day-to-day support for desktop VTC units, to include the installation, configuration, testing, debugging, and removal of these units.

The tasks in this area include:

- Install, configure, test, debug, and remove desktop VTCs.
- Periodically recommend lifecycle upgrades to desktop VTCs and, once approved and purchased, upgrade identified desktop VTCs no more than 90 days after the receipt of replacement units.

7.1.5 Telephony Instruments (Secure and Non-Secure VoIP, Secure and Non-Secure Plain Old Telephone Service (POTS))

USSOCOM, its Component Commands, TSOCs, and deployed forces provide personnel desktop telephony instruments for communication with users both inside and outside their organizations. These instruments may either be non-secure devices or secure devices that operate at one of multiple classification levels. They include Defense Switched Network (DSN) phones, secure equipment (e.g., Secure Telephone Unit (STU), Secure Telephone Equipment (STE)), secure and non-secure Voice over Internet Protocol (VoIP) units, as well as standalone telephony encryption devices (e.g., Omni, etc.).

The tasks in this area include:

- Provisioning telephones
- Configuring VoIP telephones for use with an associated call manager
- Maintaining COMSEC cleared personnel with COMSEC courier authorization.
- Keying secure equipment

- Connecting telephones to the appropriate physical network
- When applicable, changing the user name displayed on the telephone
- Enabling and disabling extension mobility
- Activating and deactivating telephone features (e.g., headsets or speaker phone functionality)

7.1.6 A/V Support for Events

From time-to-time USSOCOM, its Componet Commands, TSOCs, and deployed forces' host large meetings and forums. These events typically require some mixture of A/V equipment, to include Liquid Crystal Display (LCD) panels, speakers, microphones, soundboards, public address systems, and other devices used to make A/V presentations. The Contractor shall plan, design, setup, configure, operate, debug, and remove A/V equipment required to support these events.

The tasks in this area include

- Plan, design, setup, configure, operate, debug, and remove A/V equipment required to support large meetings and forums both within USSOCOM, Component Command, TSOC, and deployed forces' facilities, as well as at locations in and around the surrounding metropolitan area.
- Periodically setup and test A/V equipment used to support large meetings in order to verify its functionality. The Contractor shall document any failures discovered during the testing process and deliver a detailed report to the appropriate Government entity listing those failures with recommendations for addressing them.
- Periodically recommend lifecycle upgrades and improvements to A/V equipment used for large meetings and implement these once approved by the appropriate Government entity.

7.2 Common Workgroup Devices

The Contractor shall manage and support devices installed and provided for shared usage by two or more personnel (i.e., Common Workgroup Devices). Common Workgroup Devices include network-attached items, such as printers, scanners, copiers, digital senders, and multi-function devices.

7.3 Common Area VTC Equipment

The Contractor shall install, configure, manage, maintain, operate, and defend VTC equipment, including day-to-day setup, scheduling, and monitoring. This includes fixed Conference room based VTCs, desktop VTC suites, portable VTC suites, and associated VTC equipment (e.g., dedicated VTC Coder-Decoders (CODECs), dedicated VTC video cameras, video walls, video cubes, projectors, projection screens, LCD panels, speakers, microphones, audio equipment, Biamp Digital Signal Processing (DSP) equipment (to include supporting and maintaining dedicated Biamp firmware), soundboards, control consoles, Digital Media (DM) A/V switching systems, touch panel control firmware, etc.). The Contractor shall perform initial installation, connection, configuration, and adjustment, as necessary. Additionally, the Contractor shall provide operational assistance (via A/V personnel on-site at the user's location) for conducting video teleconferences.

The tasks in this area include:

- Provide dedicated on-site support at USSOCOM, Component Command, TSOC, and deployed forces' facilities, to include events occurring at off-site locations.
- Schedule, coordinate, and administer multiple simultaneous VTC sessions.
- Provide dedicated support to VTCs attended by Very Important Persons (VIPs), including setup, real time monitoring, troubleshooting and tear down.
- Recommend upgrades to VTC systems at least annually and incorporate approved upgrades when acquired.
- Provide version control and provisioning, via TMS, for VTC CODECs.
- Install flat panel displays, room-based VTC endpoints, projectors and A/V equipment.
- Accomplish associated A/V and VTC troubleshooting, to include touch panel control subsystems. Resolve issues down to the equipment level (black box).
- Manage, maintain, and post a daily Master Station Log (MSL) and shift change procedures to ensure proper information flow across shifts. This MSL shall provide a record of maintenance requirements, functions, and corrective actions taken. The Contractor shall document when the deficient function or operation was first discovered or reported, the exact time it was corrected, and when the service, function or operation was restored.
- Schedule, configure, and connect users to DISA Global Video Services (GVS) and DVS conferences.
- Train designated personnel on the operation of VTC equipment.
- Maintain COMSEC cleared personnel with COMSEC courier authorization and the ability to key USSOCOM's secure VTCs.

7.4 End User Mobile Computing Devices

The Contractor shall provision, manage, maintain and track end user mobile computing devices (e.g., non-secure and secure handheld mobile devices, smartphones, and other handheld communication devices) authorized by USSOCOM, its Component Commands, TSOCs, and deployed forces and assigned to individual personnel for secure and non-secure communications. The Contractor shall coordinate device configuration, allocation, and provisioning for devices that utilize services offered by external providers (e.g., secure Blackberry devices). The Contractor shall maintain mobile computing devices, draft mobile computing policies and procedures, implement and integrate new mobile computing services and technologies, as well as troubleshoot, repair, and provide logistical support for existing devices.

The tasks in this area include:

- Designate a primary and alternate mobile device manager in accordance with the SIE OPORD, update the list of mobile device managers as changes occur, and notify USSOCOM, its Component Commands, TSOCs, and deployed forces within one business day of any changes to the list.
- Prepare, configure, test, troubleshoot, issue, and receive mobile communications devices and associated auxiliary devices.
- Provide personnel cleared to act as a COMSEC Responsibility Officer to perform the following activities:
  - Add and remove COMSEC keys
  - Manage COMSEC key inventory
  - Destroy COMSEC keys

    - Manage COMSEC Digital Management Devices (DMDs)
    - Control physical access to COMSEC
- Interface directly with customers to provide training and to resolve issues related to services.
- Maintain mobile computing device utilization history, to include a review of device and service usage, audits, and reconciliation of utilization.
- Baseline and maintain end user mobile computing device configurations, including STIGs, and maintain configuration control and policy management of devices.
- Configure and maintain mobile computing devices in accordance with USSOCOM, Component Command, TSOC, deployed forces' and DoD Cybersecurity policies, procedures, regulations and directives.
- Coordinate and manage accountability of new equipment, replacement equipment, and upgrades. The Contractor shall track the disposition of equipment throughout its life cycle (e.g., CERP and LCR).

8.0 Plans and Engineering

USSOCOM has a plans and engineering capability for both integrating new hardware and software into its existing baselines and for identifying and documenting new solutions and candidate technologies for future adoption. The Contractor shall support USSOCOM plans and engineering by providing personnel and subject matter expertise to USSOCOM integration facilities, as well as architects and engineers to recommend new applications and technologies for adoption.

8.1 SOF Integration Facility (SIF)/Site Integration Team (SIT)

The USSOCOM SOF Integration Facility (SIF) is a comprehensive IT hardware and software integration resource and test environment enabling objective technical and functional assessments of SIE requirements. It is an area available to USSOCOM and its Contractors that allows the integration of hardware and software in an environment isolated from the enterprise operational IT network.

The Contractor shall use the SIF to install, test, package, and document new capabilities for the SIE. The Contractor shall also install, integrate, configure, secure, monitor, update, document, manage, and maintain SIF server, storage, and network infrastructure to enable the SIF to continuously provide an adequate and secure test and integration environment for USSOCOM. This includes the timely application of approved cybersecurity patches software and software updates to SIF hardware and software.

In addition to addressing enterprise capabilities, the Contractor shall, as directed, coordinate and collaborate with the Site Integration Teams (SITs) at USSOCOM Component Commands and TSOCs and assist them with the integration of site specific software into the enterprise software baseline. The Contractor shall also apply approved cybersecurity patches and software updates in a timely manner to SIT hardware and software.

8.2 Software Baseline Management

The Contractor shall provide and manage enterprise-wide lifecycle Software Image Management Services for USSOCOM Core Images and designated above baseline applications. This includes the activities and tasks associated with defining, building, configuring, testing, deploying, verifying, monitoring, revising, archiving, maintaining, updating, patching, and controlling changes to Core Images and above baseline applications that are deployed for use on computing devices. The Contractor shall provide remote administration,as well as patch distribution and management. At any given time, the USSOCOM enterprise uses, supports and maintains multiple Core Images which the Contractor is required to support.

The tasks under this area include:

- Perform enterprise-wide lifecycle Software Image Management for USSOCOM software baselines and create new baselines in accordance with USSOCOM policies, procedures, regulations, and directives.
- Create and update software baselines for USSOCOM, in accordance with the frequency specified in USSOCOM policies, procedures, regulations, and directives.
- Define, build, configure, test, deploy, verify, monitor, revise, archive, maintain, update, patch, and control changes to software baselines that are built and deployed for use on computing devices, including servers and end user desktops.
- Incorporate USSOCOM approved IAVAs, STIGs, and vendor-supplied software updates into software baselines created, unless directed otherwise by USSOCOM.
- Manage, maintain, and periodically update the USSOCOM Validated Product List (VPL) in accordance with USSOCOM policies, procedures, regulations, and directives.
- Serve as the subject matter expert (SME) on the USSOCOM baseline and VPL, providing recommendations and courses of action on software rationalization.
- Create, build, update, and maintain a USSOCOM approved collection of software installable on demand by end users (i.e., "app store").

8.3 Release Management

The goal of Release Management (RM) is to deploy releases into the production environment with minimal to no disruption to either enterprise or local services as a result of errors caused by the release packages. Additionally the Contractor shall continually improve their ability to deliver changes and releases faster and at an optimum cost while minimizing risk to the operational environment and avoiding service outages. The Contractor shall develop, implement, update, and monitor RM processes for implementing approved changes to defined IT services, software and hardware. The Contractor shall use a holistic approach to develop RM processes and methodologies.

The tasks in this area include:

- Develop, implement, update, and monitor RM processes for implementing approved changes to defined IT services, software, and hardware.
- Develop and use a holistic approach in creating RM processes and methodologies.
- Ensure that technical and non-technical aspects of a release are taken into consideration in designing and building the release.
- Plan and perform the release of approved software, hardware, policy, and procedural changes.
- Perform RM activities related to preparing new or reconfigured software and hardware for release.
- Adhere to USSOCOM RM policies, procedures, processes, and regulations for implementing approved changes to the enterprise, including software and hardware.
- Through the use of various technologies, socialize technology changes impacting

USSOCOM to its end users, focusing on benefits and expectations.

- Collaborate with other support teams which are directly affected or impacted by RM activities including: Change Management, Configuration Management, Problem Management, Consolidated Service Desk (CSD), production operations, and other pertinent IT support groups relating to release training for system administrators, release content, schedule, and approval.
- Develop and update release implementation plans to cover Operational Test and Evaluation (OT&E), training operations teams and the CSD, and testing transition of the release to the production environment. Ensure that each release and release packages can be tracked, installed, verified, and uninstalled or backed out if required.
- Create an approach for building, testing and maintaining controlled OT&E environments with activities including:
    - Developing build plans from design specifications and environment configuration requirements
    - Establishing the logistics, lead and build times to set up the environments
    - Testing the build and related procedures
    - Scheduling the build and test activities
    - Assign contractor resources, roles and responsibilities to perform key activities
- Incorporate a categorization methodology into the Release Management process to include the following release levels:
    - Major software Releases and hardware upgrades
    - Minor software Releases and hardware upgrades
    - Emergency software and hardware upgrades
    - Software Patches
    - Post Implementation Review

8.4 Projects

The Contractor shall provide a project team having the skills necessary to execute transition activities to field new capabilities into the SIE. The project team will assist the operations and management team with project planning, installation, operation, and maintenance of new capabilities, as required, before requesting USSOCOM approval for official release. The project team shall produce required build documentation and training materials, as well as test the environment to ensure a smooth transition to the operations and maintenance team. USSOCOM, its Component Commands, TSOCs, and deployed forces will define and prioritize the list of projects that the Contractor shall accomplish. The Contractor shall provide the following documents for each project:

- Implementation Plan (CDRL A005)
- Interface Design Description (CDRL A006)
- Performance Specification Documents (CDRL A007)

A project is a USSOCOM, Component Command, TSOC, or deployed forces' designated and approved activity, or group of activities, required to achieve an objective. A project is also a set of related tasks that are undertaken to create, provide, deliver or enhance a specific IT product or service. Each project has a lifecycle that typically includes initiation, planning, execution and closure, and is usually managed by a formal methodology. Standard installations, moves, adds, and changes (IMACs) do not fall within the definition of a project.

The tasks under this area include:

- Manage projects using industry best practices.
- Provide a technical assessment of potential new services and capabilities per the policies, procedures, regulations and directives of USSOCOM, its Component Commands, TSOCs, and deployed forces.
- Scope new projects, identify capability gaps (e.g., lack of required software and hardware), propose COAs for accomplishment, and define long term sustainment requirements (people, processes, technology, training, Cybersecurity).
- Serve as SME/Tier 4 support for USSOCOM, Component Command, TSOC and deployed forces' services and capabilities throughout their lifecycle.
- Perform integration of new services and capabilities.
- Support and assist the O&M of new services and capabilities during a transition timeframe approved by USSOCOM, its Component Commands, TSOCs, and deployed forces.
- Create and deliver necessary documentation for new services/capabilities, to include:
    - Assessment and Authorization (A&A) packages
    - Architecture
    - Configuration data
    - Software description document
    - Licensing

8.5 Architects and Engineers (A&E)

This section identifies the specific subject matter experts (SMEs) required by USSOCOM to enhance their IT planning for future operations. These individuals will have superior knowledge in general systems engineering, as well as specific fields of expertise, and be adept with IT, major datacenter operations, and network defense. Unless otherwise directed by USSOCOM, contractor personnel will be assigned to HQ USSOCOM, MacDill Air Force Base, FL., but they may be required to perform some travel in both CONUS and OCONUS. All personnel proposed for the identified SME requirement under this section are considered key personnel.

A&E personnel shall not perform day to day operations support or project development, but will act in an engineering/architectural planning capacity while occasionally performing Tier IV SIE support functions. Individuals provided will be responsible for interfacing with O&M personnel and providing strategy and direct design support to USSOCOM projects. Personnel will periodically review existing architectures, recommend improvements, and attend planning, O&M, and engineering meetings that require their expertise.. Individuals provided will have full administrative access over their specific areas of expertise in the operational environment. Individuals shall perform their duties during normal USSOCOM business hours with occasional emergency after hours support.

Specific functional areas requiring SMEs are:

- General systems engineering with a focus on the end-to-end functionality of complex systems of systems
- Messaging with expertise in Microsoft Exchange 2010+, Microsoft Lync 2010+, Cisco Jabber, Cisco Video Teleconferencing, and messaging service integration.
- Database with expertise in Microsoft SQL, Oracle, and Microsoft JET.
- Thin Client and Virtual Desktop Infrastructure (VDI) with expertise in Citrix and VMware thin client solutions.

- Directory Services/DNS with expertise in Microsoft Active Directory, Microsoft DNS and Infoblox.
- Storage with expertise in Storage Area Networks technologies, Network Attached Storage technologies, iSCSI, and Direct Attached Storage technologies with an emphasis on EMC and NetApp solutions.
- Portal/Web with expertise in the design of medium to large enterprise Microsoft SharePoint 2010+ farms, geographical replication, interfacing with external data sources and integration of third party add-ons.
- Public Key Infrastructure (PKI)/Certificate Authority Services with expertise in Microsoft Certificate Services and Terminal Access Controller Access-Control System (TACACS).
- Customer Relationship Management (CRM) (Microsoft Dynamics CRM).
- Disaster Recovery and backup/restore with expertise in Symantec NetBackup and EMC products including Data Domain.
- Virtualization with expertise in VMWare.
- Cybersecurity technology, risks and risk mitigation strategies related to cybersecurity, and A&A support documentation IAW applicable DoD and IC directives.
- LAN, WAN and VoIP infrastructures, voice and data network systems, advanced engineering and administration of multiprotocol routers, multilayer switches, network security devices and network management systems.
- Satellite communications with an emphasis on IP satellite technology.
- Application Delivery Networking technology with an emphasis on products from F5 Networks, Inc.
- Cloud computing technology
- Mobile computing technology
- Desktop computing technology
- Tablet technology
- Wireless networking technology
- SATCOM technology

9.0 Enterprise Architecture (EA)

The USSOCOM CIO establishes plans, policy, and direction for the entire USSOCOM Enterprise. Key functions of this office include establishing and documenting the Enterprise Architecture of the SIE and capability architectures supporting the Joint Capabilities Integration Decision System (JCIDS) and SOF Capabilities Integration Decision System (SOFCIDS) processes. This provides a target for the rest of USSOCOM to build their IT acquisition roadmaps against. The Contractor's primary support to the CIO is through the research, design, and development of Enterprise Architecture products, primarily using the DoD Architecture Framework (DoDAF).

Contractors performing USSOCOM EA tasks shall provide overall DoDAF/JCIDS/SOFCIDS situational awareness to the Enterprise. The Contractor shall assist with the operations and maintenance of Enterprise Architecture tools, including the administration and backup of any associated databases. The Contractor shall also create, publish, and post architecture products on both USSOCOM and Joint portals. Note that the Enterprise Architects described in this section are distinct and different from those described in Section 8.5, "Architects and Engineers," have very different knowledge and skill sets, and do not perform the same activities.

The Contractor shall provide EA staff with superior knowledge in their individual fields, as well as familiarity with other areas of USSOCOM core operations (e.g. foreign internal defense, unconventional warfare). EA Contractor personnel shall not perform day-to-day operations support or project development, but shall act in a planning capacity. The Contractor shall collaborate with the DoD CIO, IC, Joint Staff, Military Services, DISA, Component Commands, TSOCs, and USSOCOM personnel to create the EA and capability architectures. This includes reviewing new capability architectures or guidance proposed by the above organizations for the impact of those capability architectures upon the SIE. When USSOCOM, its Component Commands, or its TSOCs propose new capability architectures, the Contractor shall evaluate them for compliance with Joint and USSOCOM architecture standards.

Included in the Contractor's support to EA is EA staff located at each USSOCOM Component Command. The standards for these Component-based EAs are identical to those for the USSOCOM Enterprise outlined above. Co-locating this staff at each Component allows the Component Commander to redirect and prioritize the Contractor to focus on DoDAF/JCIDS/SOFCIDS products based upon the Component Command's mission priority. However, these Component EAs are not independent elements and must collaborate with USSOCOM Enterprise architects to ensure standardization.

The Contractor shall provide support during duty hours at their assigned location and may be required to perform some travel in both the CONUS and OCONUS to locations such as Washington, D.C., HQ USSOCOM, Component Commands, TSOCs, and other locations deemed necessary by USSOCOM.

The tasks under this area include:

- Understand USSOCOM strategies, missions, roles, and functions and perform mid- and long-term Enterprise and strategic C4 planning based on this understanding.
- Understand and use the DoDAF, JCIDS, SOFCIDS, and other key DoD/Joint architecture planning instructions.
- Create and maintain the EA using DoDAF architecture products and supporting documentation.
- Create and maintain DoDAF architecture products and supporting documentation for submission to and approval by the Special Operations Command Requirements Evaluation Board (SOCREB).
- Create and maintain DoDAF architecture products and supporting documentation for submission to and approval by the Joint Requirements Oversight Council (JROC).
- Create and maintain DoDAF architecture products which also comply with the DoD Business Enterprise Architecture standards for submission to and approval by the DoD Deputy Chief Management Officer investment review boards
- Create and maintain "fit for purpose" products, which may be a single DoDAF product or a combination of product types to address CIO issues/events.
- Use of a variety of DoD, Joint Staff, Military Service, DISA, and IC resources/sites to create the EA and capability architectures. These resources include the Architecture Compliance and Assessment Review Tool (ACART), the Universal Joint Task List (UJTL) Task Development Tool, and the GIG Technical Guidance-Federation.
- Review and assess the impact of DoD, Military Service, Joint, DISA, or IC proposed capability architectures or architecture guidance on the SIE.
- Upload USSOCOM products and maintain the USSOCOM section of the Warfighting Mission Area Architecture Integration Portal on SIPRNet and NIPRNet

- Administer the USSOCOM architecture software and database
- As requested, participate in DODAF related conferences, either virtually or in person.
- Capture the current, "as is" architecture for each USSOCOM Enterprise service and create logical and physical maps of each service.
- Create comprehensive logical and physical "as is" maps of USSOCOM data centers, Regional Support Centers (RSCs) and networks.

10.0 Configuration, Change, License, and Asset Management

In order to maintain configuration standards, control changes, and properly track and account for both IT equipment and software, USSOCOM needs to rigorously execute configuration, change, license, and asset management. Configuration management ensures that performance of IT-enabled services and capabilities remains consistent with service design by defining, documenting, and tracking the functional, physical, and relationship attributes between key resources and attributes necessary to deliver the service, including defining service standard attributes for systems on the USSOCOM network, controlling changes to these standards, and verifying and maintaining standards through auditing and remediation. Change management provides knowledge and control of Who did What, When, Where, and Why, at any point where change occurs throughout an IT system lifecycle, as well as manages requests for the introduction of new hardware or software. License management tracks the acquisition, allocation, assignment, installation, and removal of software licenses in inventory and deployed to operational systems, ensuring USSOCOM compliance with software license agreements. Asset management tracks, records, and accounts for physical IT equipment managed or deployed in support of SOF, ensuring full accountability for equipment under USSOCOM control. These processes together allow USSOCOM to maintain a complete and accurate view of its network and system configurations, lifecycle states, software and licenses, and IT equipment.

10.1 Configuration Management

The Contractor shall follow an IT service based approach to manage, monitor, and update USSOCOM Configuration Management (CM) Data in the CM database (CMDB) and the CM document library (CMDL), including a logical service model of enterprise devices and their relationships by identifying, controlling, maintaining and verifying installed hardware, software, and documentation (e.g., Architecture, Server Build, System Installation documents as well as maintenance contracts, SLA documents, etc.). The Contractor shall periodically verify configuration records against the infrastructure and defined service standards and correct any exceptions.

The tasks in this area include:

- Propose improvements to the USSOCOM Configuration Management Plan and deliver them to the USSOCOM Configuration Manager no more than 90 calendar days after task order award.
- Create "as is" build documentation for each service no more than 60 calendar days after Task Order award.
- Update service/configuration item build documentation no less than every 60 calendar days.
- Install, update, maintain, and decommission Configuration Management tools.
- Enter/upload and maintain configuration data into the CMDB.

- Create, maintain, and update logical service models.
- Maintain Configuration Management records for USSOCOM directed Configuration Items.
- Recommend additional attributes for service/standard drift capability.
- Create and maintain service and inter-service Configuration Item relationships.
- Establish and maintain process interfaces to Incident and Problem Management, Change Management, and Asset Management processes.
- Establish appropriate authorization controls for modifying configuration items.
- Establish procedures for verifying the accuracy of Configuration Items, adherence to the Configuration Management process, and identifying process deficiencies.
- Provide Configuration Management reports in compliance with USSOCOM policies, procedures, regulations, and directives.
- As required, recommend updates and changes to Configuration Management reports.

10.2 Change Management

The Contractor shall manage, monitor, and update the enterprise-wide Change Management process when introducing any change into the IT production environment. The Contractor shall recommend and, when approved, execute standardized methods and procedures for the efficient and prompt handling of IT Service Requests for standard and non-standard change (e.g., submitting, reviewing, prioritizing, approving, recording, managing the processes, etc.) in order to minimize any negative impact of change to availability or quality of the service. The Contractor shall also ensure that the Change Management processes include interfaces to the Release Management, Configuration Management, Asset Management, Incident Management, Problem Management, and NetOps processes.

The tasks under this area include:

- Recommend and then utilize an approved change priority schema with classifications (impact, priority, risk) and a change authorization process that align with USSOCOM, Component Command, TSOC, and deployed forces' requirements.
- Maintain, manage, and update a Request for Change (RFC) status register that is used to record, track, and report on the status RFCs submitted for consideration.
- Receive and document RFCs and classify proposed changes to the services, which shall include the cost of the change, a risk impact assessment, and any system(s) security considerations.
- Propose improvements to the enterprise Change Management plan to the USSOCOM Change Manager for review no more than 60 calendar days after task order award.
- Develop and maintain a schedule of planned, approved changes (Forward Schedule of Changes or FSC) for USSOCOM to review.
- Provide change documentation, as required, including proposed metrics for measuring the effectiveness of a change.
- Publish and communicate the approved FSC to appropriate IT and mission personnel according to USSOCOM policies and procedures.
- Monitor changes, perform change reviews, and report results of changes, impacts, and change effectiveness metrics.
- Verify that changes meet objectives based upon predetermined effectiveness metrics, and determine follow-up actions to resolve situations where the change failed to meet objectives.

- Identify and report to USSOCOM approved RFCs that have been cancelled or otherwise abandoned.
- Close out RFCs that met the change objectives.
- Close out abandoned RFCs with USSOCOM approval.
- Coordinate, schedule, and facilitate Change Board meetings, to include the review of planned changes and results of changes made, ensuring that appropriate parties are invited and represented in accordance with approved USSOCOM policies and procedures.
- Document the relationship of changes to Configuration Items and services.
- Perform an analysis of change related incidents and provide a report to USSOCOM according to USSOCOM policies and procedures.

10.3 License Management

The Contractor shall operate a software inventory management program to ensure compliance with DoD policy, Federal laws, and industry best practices. The Contractor shall monitor, track, and ensure that software in use on USSOCOM networks that requires a license is licensed and, when appropriate, has maintenance agreements in the CMDB and in the Software Document Library (SWDL). The Contractor shall consider usage trends, migration plans, operational changes, and return on investment (ROI) when researching alternatives. The Contractor's program shall maximize ROI and maintain the warranty and maintenance coverage for hardware and software (including Contractor-purchased items and USSOCOM-purchased items).

The tasks in this area include:

- Provide dedicated on-site support for enterprise software license management.
- Monitor and manage USSOCOM's centralized data repository for enterprise-wide use to record and track information regarding software licensing meta-data and support agreements (e.g., vendor name, software name and version, number of authorized users and devices covered, number of users currently using the software, licensing fees, commencement and expiration date, etc.).
- Track licenses, maintenance plans, renewal information, and media for software owned by USSOCOM, its Component Commands, TSOCs, and deployed forces.
- Report to the USSOCOM Software Manager any exceptions to vendor terms and conditions, including license non-compliance.
- Perform a periodic review of software license and maintenance agreements and provide a monthly report with any findings.
- Coordinate software license and maintenance agreement reviews with the USSOCOM Software Manager and SOF Acquisition, Technology, & Logistics (AT&L) within 120 days of expiration.
- Advise the USSOCOM Software Manager on software acquisition and discontinuation decisions.
- Help the USSOCOM Software Manager maintain software license compliance by recommending either the acquisition of additional licenses or curtailing usage, whichever is appropriate based on the applicable data.
- Identify, document, and report license compliance issues to the USSOCOM Software Manager and recommend appropriate action.
- Perform periodic software license audits, reconciling the number of licenses utilized to the number owned by USSOCOM, its Component Commands, TSOCs, and deployed forces.

- Hold periodic software license reviews and ensure reviews are conducted 120 days prior to the expiration of software license and maintenance agreements, and provide monthly reports on the status of license expirations.
- When software license reconciliation issues arise, recommend mitigations to these issues to the USSOCOM Software Manager.

10.4 Asset Management

USSOCOM, its Component Commands, TSOCs, and deployed forces require Inventory Control Analysis support to maintain consistent accountability of ADPE assets supporting the SIE. The Contractor shall perform shipping and receiving of ADPE assets, accountability of inventory in USSOCOM,Component Command, TSOC, and deployed forces' short term storage facilities of computer/communications-related assets, and distribution of hardware in conjunction with USSOCOM-delivered distribution plans at HQ USSOCOM, its Component Commands, TSOCs, and deployed forces. The Contractor shall ensure that ADPE hardware and software are properly received in an Accountable Property System of Record (APSR)-approved database, documented in accordance with Personal Property Management (PPM) requirements, stored, and disbursed to the required user to maintain good supply and accountability of ADPE.

The tasks under this area include:

- Provide dedicated on-site support during duty hours.
- Develop and maintain approved processes for managing and tracking the full IT asset, license, and maintenance life cycle from procurement to retirement.
- Define, maintain, and update approved policies and procedures for effective asset life cycle management (acquisition, deployment, utilization, de-installation, reallocation and disposal) of IT assets.
- Schedule and revise shipment plans to ensure efficient distribution of products to satisfy customers. Analyze inventory levels and product demand to determine reorder levels, which shall ensure product availability and minimize inventory costs.
- Manage inventory levels to efficiently utilize capital investment while maintaining adequate coverage for known/projected demand.
- Maintain control and accountability over assigned products; determine appropriate distribution based on lead times and demand.
- Ensure property items are uniquely identified and changes are tracked and recorded in accordance with PPM requirements. Ensure property items are uniquely identified and changes are tracked and recorded.
- Inspect goods and materials and assess condition for distribution/recycling.
- Coordinate the disposal of property, supplies, and materiel in compliance with USSOCOM and Service regulations/guidelines.
- Maintain records of acquisition/distribution of property, supplies, and materials. These records will include, at a minimum, the following forms, as applicable: DD Form-1149, DA Form-3161, SF-153, DD Form-1155, DD Form-250.
- Process excess ADPE as identified by USSOCOM using DoD procedures.
- Aid USSOCOM with completing quarterly and annual inventories while ensuring no less that 90% accuracy of the CMDB.
- Define metrics, gather data, and report on the effectiveness of IT asset management processes

10.5 IT Service Management Suite

A robust enterprise IT Service Management program ensures that key and supporting services are consistent with service design and performance standards throughout the service lifecycle. As such, the Contractor shall establish and operate a USSOCOM provided IT Service Management program that incorporates Incident, Problem, Service Request, change, configuration, and asset management processes for services on USSOCOM networks. The Contractor shall also operate and maintain the ITSM system suite, advising USSOCOM on optimizations, upgrades, design and architecture, new functionality, and enhancements, as well as developing system enhancements to support business metric reporting and established business processes (e.g., workflows, active links, customer forms, and objects).

The Contractor shall demonstrate expertise with the following IT Service Management concepts, methodologies, services and technologies:

- User facing and technical Service Catalog management, to include recommending and implementing new standard services, standard service design, and workflow development.
- ITSM suite integration and web service connections to databases, websites, and portals
- Service modeling, mapping and CMDB population to include network scanning for configuration item discovery (e.g., additions, deletions, exclusions, etc.).
- Maintanence of a 95-99% accurate CMDB.
- Integration of the ITSM suite with other IT management tools owned by USSOCOM to allow the proper flow of information between tools to include BMC Remedy, Microsoft SharePoint, Microsoft System Center Configuration Manager (SCCM), and Cisco Network Configuration Manager.
- Periodically merge data from multiple sources into the CMDB using reconciliation jobs per USSOCOM policies and procedures.
- Provide training on USSOCOM ITSM Processes and ITSM tools
- Manage service request entitlements and process definition templates.
- Manage the process and assignment workflow for Incident and Change Fulfillment records, including the configuration of advanced assignment rules, task phasing, and Change Request status flows.
- Manage the mapping of attributes between external asset data sources and the CMDB
- Create, delete, and manage ITSM user accounts, groups, and permissions.
- Manage ITSM foundation data (e.g., organizations, departments, sites, site groups, permission groups, etc.).
- Perform ITSM troubleshooting and root cause analysis, and recommend solutions to USSOCOM when issues arise.
- Establish, maintain, and validate, through testing, a disaster recovery process and COOP plan for the ITSM suite.
- Provide, upon request, an export from the CMDB, using rconciliation jobs, to support the importing and updating of data into other DoD, Component Command, TSOC, and deployed forces' asset management systems.

11.0 IMACs

The Contractor shall perform IMACs for USSOCOM, Component Command, TSOC, and deployed forces' IT hardware and software in response to Service Requests. This shall include the installation, relocation, upgrade, change, modification, reconfiguration, and secure disposal of hardware and software. The Contractor shall provide support for IMAC requests as part of normal day-to-day operations.

The tasks in this area include:

- Conduct pre-installation and site survey activities (e.g., requirements gathering, assessments, preparing equipment list(s), obtaining quotes, coordinating with third-parties and other organizations, ensuring network connectivity to appropriate networks, power, data, voice, and video wall jack preparation) in accordance with USSOCOM procedures and the requirements of the associated Service Request. Upon completion of these site surveys, the Contractor shall report the results to the requesting organization.
- Build, configure and test IT equipment in accordance with USSOCOM's standard hardware configuration(s), software Image(s), procedures, and specific requirements outlined in the associated Service Request.
- Perform hardware and software IMACs and re-installations in accordance with the associated Service Request requirements, and other applicable USSOCOM procedures and policies (e.g., security policies, property accountability policies).
- Conduct application and data migration necessary as a result of a hardware or software IMAC or re-installation.
- Update relevant cross-functional management tools (e.g., asset management database, drawings, etc.) with required data upon closure of an IMAC Service Request.
- Provide basic end user or technical personnel orientation, as needed, when installing a new desktop computing device and associated peripherals (e.g., thin client, desktop or laptop).
- Coordinate with the USSOCOM CSD, the requesting organization, and other necessary IT service providers, third-parties, and support organizations to manage IMAC Service Requests to resolution and closure.