# PERFORMANCE WORK STATEMENT

# for

# United States Air Forcesin Europe and Africa

# (USAFE-AFAFRICA)

INFORMATION TECHNOLOGY SUPPORT SERVICES
(ITSS)
Model Task Order PWS - EUROPE-WIDE IT ENTERPRISE

NETWORK SERVICES (EITEN)
FA5641-22-F-XXXX
29 Sept 2021

## Table of Contents:

# PERFORMANCE WORK STATEMENT (PWS)
# INFORMATION TECHNOLOGY SUPPORT SERVICES (ITSS)

## 1. Introduction:

**1.1. Goal:** The goal of this contract is to provide non-personal services in support of the HQ USAFE-AFAFRICA Communications Directorate’s (hereby referred to as A6) missions to enable combatant command (CCMD) directed operations and exercises; operate and sustain major command (MAJCOM) unique information technology (IT) systems; and meet Department of Defense (DoD) and United States Air Force (USAF) goals to improve IT effectiveness and efficiency. To support this vision, A6 has been at the center of incorporating advanced technologies that enable new operational concepts and the information warfare. In order to achieve this goal and to continuously outpace the Nation’s adversaries, A6 has established primary objectives to achieve its mission and the services, and under this PWS will provide the support to achieve this goal. Core support skills required include requirements analysis, technical solution development, theater-wide engineering, cybersecurity, architecture and integration of various regional systems that support roughly 40,000 USAFE-AFAFRICA personnel with communications support.

**1.2. Mission:** A6 provides communications and information strategic direction, policy and resources for USAFE-AFAFRICA forces supporting the U.S. European Command (USEUCOM), U.S. Africa Command (USAFRICOM), North Atlantic Treaty Organization (NATO), unified commanders, coalitions, and Aerospace Expeditionary Forces. The A6 ensures these global forces have integrated, responsive, and reliable command and control, intelligence, and combat communications support during wartime, operations other than war, contingencies, exercises and daily operations. A6 supports the USAFE_AFAFRICA’s Commander as the principal advisor for cyberspace operations and issues. A6 is the coordinator for employment of cyberspace capabilities to integrate cyber with other non-lethal/lethal effects. A6 serves as advocate for organizations and agencies for cyberspace support to air and space components operations. A6 supports all these missions with forward-based airpower and infrastructure to conduct and enable theater the global operations, while at the same time operate and maintain MAJCOM systems and networks. HQ USAFE-AFAFRICA/A6 executes USAF, USEUCOM, and USAFRICOM missions by providing information dominance capabilities in cyberspace to enable base, theater, and global operations. A6 requires very broad technical skill sets and is a multi-disciplined organization that provides expertise, planning and coordination, and guidance for communications and information systems and services for USAFE-AFAFRICA.

**1.3. Scope:** This contract will allow for greater speed, flexibility, and accessibility in assessing and transitioning innovative technologies to meet A6 mission objectives. In support of these mission objectives the contractor shall provide research and development, systems engineering, testing and evaluation, training, operations and maintenance (O&M) and technical support to enable rapid assessment, development, demonstration, and fielding of new and emergent technologies to address current and evolving threats to our Nation’s defense systems and to enhance existing and future capabilities. This section functions as a general overview of the government’s intentions with this services support contract. The contractor (KTR) shall provide IT service center, systems engineering, cybersecurity, Mission Relevant Terrain- Cyber/mission mapping (MRT-C/MM), project management, and communications planning support for USAFE-AFAFRICA network environments.

**1.3.1. Support Locations:** The following Main Operating Bases (MOBs): Ramstein Air Base (AB), Germany; Spangdahlem AB, Germany; Aviano AB, Italy; Incirlik AB, Turkey; Royal Air Force (RAF) Lakenheath, United Kingdom (UK); RAF Mildenhall, UK; and their respective Geographically Separated Units (GSUs).

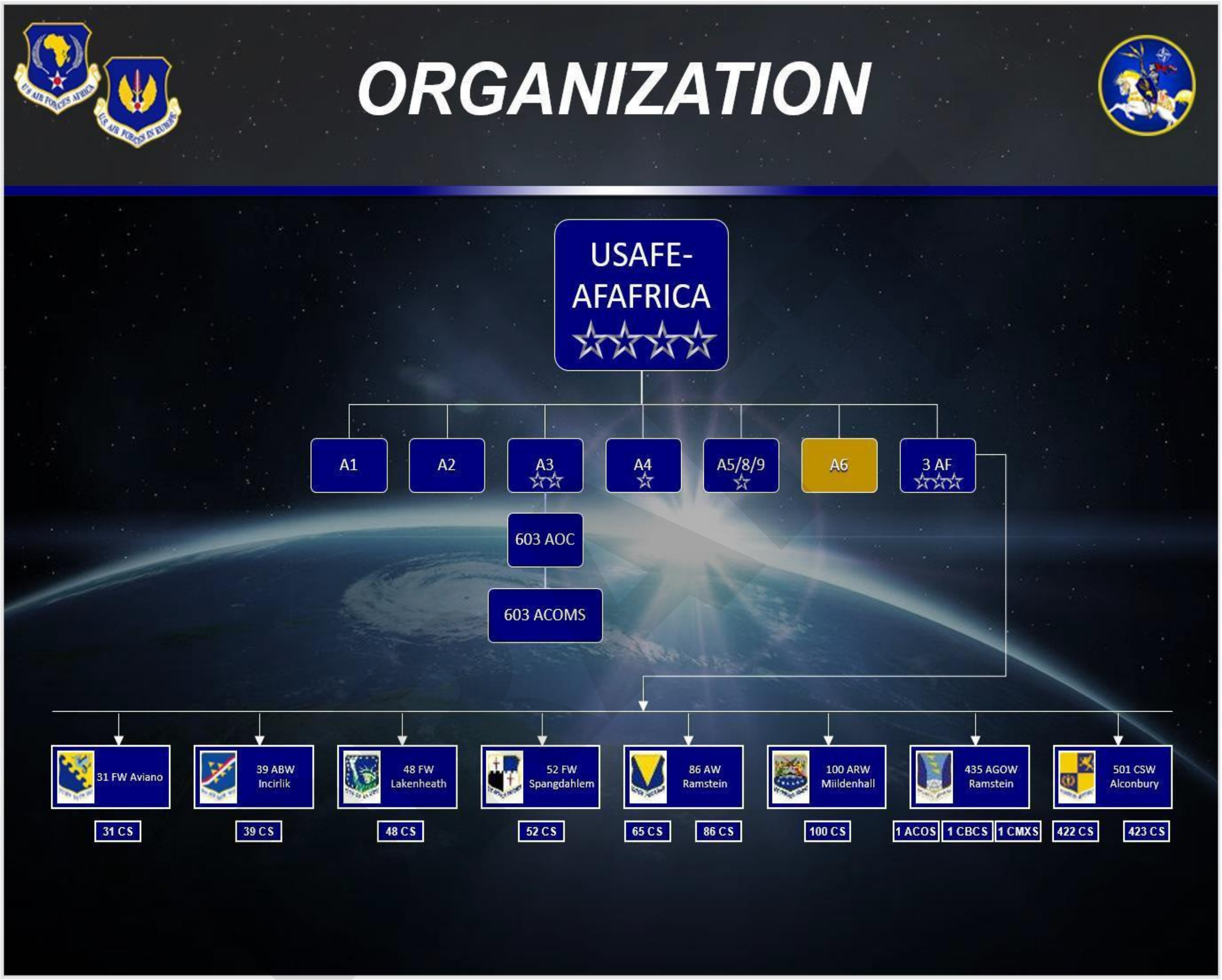


**Figure 1. Communications Organizations Structure Overview.**

**1.3.2. Tiered Operational Construct:** The delineation of the Tier Construct below is only provided for clarification on the responsibilities cited within this PWS.

1.3.2.1. **Tier 0.** This capability enables users to access automated tools (e.g., Air Force (AF) virtual Enterprise Service Desk application) solve incidents on their own (e.g., loading printers, updating global address list entries, etc.). There is currently no requirement for Tier 0 support in this PWS; however, nothing precludes the KTR from developing and/or fielding a Tier 0 tool to improve efficiency and effectiveness. Issues that cannot be resolved at this tier are escalated to subsequent tiers for resolution.

1.3.2.2. **Tier 1.** This is the front-line for user aid and normally resides at the local communications focal point or communications squadron. The local technician responds to the trouble ticketing system and attempts on-the-spot resolution for end-user/client systems and accounts (e.g., desktops/laptops, government-issued mobile devices, Voice over Internet Protocol [VoIP] phones, user accounts). The trouble ticket consists of standard information concerning the incident, user, and system health. First-touch resolution is always the goal; however, if the technician determines the issue/incident is caused by a MAJCOM or enterprise-wide incident (e.g., VoIP) call manager, centralized storage, e-mail server outage, or firewall) or is an issue the Tier 1 organization cannot resolve at their level, the technician forwards the incident to the appropriate Tier 2 organization for resolution. There is currently no requirement for Tier 1 support in this PWS.

1.3.2.3. **Tier 2.** Tier 2 support is provided by Air Combat Command (ACC) organizations (for AF-level enterprise services), special maintenance teams, and MAJCOMs (for MAJCOM-unique systems or services). While Tier 1 focuses on end-user devices, systems, and accounts; Tier 2 provides more in-depth technical support for regional or enterprise-level systems or outage impacts. Tier 2 personnel are responsible for investigating elevated issues by confirming the validity of the incident and seeking solutions. Tier 2 support is a stated requirement in this PWS.

1.3.2.4. **Tier 3.** This is the final Tier in the trouble ticketing process. Tier 3 support is provided by a program management office (for programs of record), ACC/Cyberspace Capabilities Center (CCC) for AF command lead programs, product vendors, and MAJCOMs (for MAJCOM-unique systems and services). Tier 3 is the highest level of support and is responsible for assisting Tier 1 and Tier 2 personnel with the most difficult problems and issues. Tier 3 support is a stated requirement in this PWS.

**2. Requirements/Description of Services.** The KTR shall provide a wide range of technical services and solutions that support existing capabilities (e.g., infrastructure, networks, systems, and operations) and evolve those capabilities to comply with DoD, AF, and USAFE-AFAFRICA enterprise architectures. Specifically, the KTR shall provide the following non-personal services: incident/problem/change management; systems, security, and network management systems (NMS) administration; capacity management; requirements analysis; systems engineering and integration; network engineering; cybersecurity; architecture and network documentation; technical project management; configuration management; systems analysis; and communications planning. All efforts supported under this contract shall be provided in accordance with (IAW) DoD and USAF standards as applicable to the task order. Efforts under this contract will support industry best practices when not prescribed by aforementioned standards. All products (evaluations, results, plans, documentation shall be delivered to the Contracting Officer Representative (COR) or technical representative (TR) as required; or posted in accordance with , in the established timelines detailed in each subparagraph below.

**2.1. USAFE-AFAFRICA TIER 2 SUPPORT:** The KTR shall provide Tier 2/3 support for USAFE-AFAFRICA Non-Classified Internet Protocol Routed Network (NIPRNet) and Secret Internet Protocol Routed Network (SIPRNET) systems. Tier 2/3 shall support the Tier 1 organizations shown in ***Figure 1. Communications Organizations Structure Overview***, among others (e.g., SharePoint Site Collection Administrators), for resolution of issues Tier 1 organizations cannot resolve. Tier 2/3 shall be staffed during normal business from 07:30 to 16:30. Outside these hours, the USAFE-AFAFRICA MAJCOM Communications Coordination

Center (MCCC) will field all requests for support and determine if on-call support is required (para 4.2.2.).

**2.1.1. Incident, Problem, Change Support.** Document and track incidents, problems, and change requests, in the automated Government ticketing system (para 2.1.1.6.), until resolution.

2.1.1.1. Provide incident triage to include resolution when possible and reassign or escalate incidents for resolution to other technicians as necessary. Respond to outages to the Government representative on duty and maintain an on-call roster for trouble calls outside of normal duty hours. Respond to outages during duty hours within 30 minutes of notification. Respond to after-hours outages not later than 2 hours from notification. On call rosters shall be updated and/or reviewed at least monthly and posted (IAW) para 2.4.5.), on the first business day of each month (SS# 6, RR# A064).

2.1.1.2. Contact other service providers (e.g., 691 Cyber Operations Squadron [COS], base communications squadrons, Defense Information Systems Agency [DISA]) when necessary to coordinate and resolve incidents and requests.

2.1.1.3. Per MAJCOM Communications Coordination Center (MCCC) policy, notify the MCCC of all specified outages within established timeframes. Authorized Service Interruptions (ASIs) are submitted 45 business days prior to any upgrade or modification and approved 1-10 days prior to any upgrade or modification, no deviations from standard (RR#: A065).

2.1.1.4. Contact on-call personnel when required.

2.1.1.5. Monitor supported networks and systems for anomalies, incidents, and outages.

2.1.1.6. Use the government designated IT event tracking system (currently "Remedy" or any replacement system).

2.1.1.7. Verify resolution with the customer prior to closing incidents, problems, and requests.

**2.1.2. Systems Administration Tasks**. The KTR shall perform the following common systems administration tasks:

2.1.2.1. Analyze system logs and identify potential anomalies, incidents, or problems.

2.1.2.2. Introduce and integrate new technologies into existing environments.

2.1.2.3. Perform routine audits of systems and software.

2.1.2.4. Perform backups and data recovery.

2.1.2.5. Apply operating system updates, patches, and configuration changes.

2.1.2.6. Install and configure new hardware, firmware, and software.

2.1.2.7. Add, remove, or update user account information.

2.1.2.8. Answer technical queries and assist customers.

2.1.2.9. Document the system configuration and post upon notification of requirement by the COR or TR (RR#: A008).

2.1.2.10. Troubleshoot any anomalies, incidents, or problems.

2.1.2.11. Tune and optimize system performance.

2.1.2.12. Configure, add, and delete file systems.

2.1.2.13. Create, modify, change, and test continuity of operations plans (COOP) and post within 2 business days of creation or update (RR#: A036). The creating and update of the COOP requires review and approval from the COR/TR, followed by implementation upon direction from the Government.

2.1.2.14. Establish a system baseline and evaluate all system changes, upgrades, or replacements for impacts.

2.1.2.15. Build and maintain a proper staging environment that mirrors (as close aspossible) the production environment.

2.1.2.16. Test all updates or changes on the staging environment and obtain Government approval prior to implementing on the production environment.

**2.1.3. Systems Security Administration.** The KTR shall perform the following systems security tasks:

2.1.3.1. Initiate and maintain acceptable authorization and accreditation (A&A) status for managed systems. All current systems fall under the wing enclave A&A package and require supporting artifacts; however, new or upgraded systems may require their own A&A package.

2.1.3.2. Maintain all system devices (e.g., servers) IAW DISA Security Technical Implementation Guides (STIG) and U.S. Cyber Command (USCYBERCOM), Air Force Cyber Command (AFCYBER), and 16 AF taskings.

2.1.3.3. Take appropriate measures to respond to known and possible network attacks IAW applicable DOD policies, directives and instructions.

2.1.3.4. Ensure all KTR managed items are configured to store and archive allsystem, device, application, and security event logs in accordance with DoD securitypolicy.

2.1.3.5. Audit and review all system, device, application, and security event logs in accordance with DOD security policy.

2.1.3.6. Support and provide the necessary information (e.g., firewall logs, system logs, and storage media) to the computer network defense service provider and other government - designated organizations in the performance of forensic analysis services when required.

**2.1.4. Data Center and System Storage Capacity Management.** The KTR shall assist the Government in identifying and matching the storage needs of KTR operated and maintained systems to allocated storage space. Based on recurring systems administration tasks, the KTR shall assess whether there are potential storage problems and issues that must be addressed, and post the assessment results within 2 business daysof review (RR#: A049). The KTR is not responsible for providing additional storage space. The KTR shall provide the following storage capacity relatedservices:

2.1.4.1. Follow the backup and recovery plans to ensure there is no application performance degradation according to service-level agreements.

2.1.4.2. Manage allocated storage to avoid incidents caused by lack ofcapacity.

2.1.4.3. Justify and request additional storage should it become necessary, and post the document within 2 business days of completion (RR#: A050).

**2.1.5. MAJCOM-unique Supported Systems.**

2.1.5.1. **Unified Communications Support**. (Mission Essential (ME) services: 2.1.5.1. – 2.1.5.1.11.3., see para 2.4.2.)

2.1.5.1.1. **Unified Communications Call Manager.** Cisco Unified Communications Manager (CUCM) is the core of the USAFE-AFAFRICA unified capabilities (UC) platform, and it is virtually hosted on Cisco Unified Computing System (UCS) platform. The system currently supports 84 locations across Europe and Africa with 40,000 customers using 32,000 connected devices distributed among twelve call clusters. USAFE-AFAFRICA also supports 3,000 Voice over Secure Internet Protocol (VoSIP) customers on a separate call cluster. Based on the mission assigned to USAFE from higher headquarters, the above cited numbers can fluctuate.

2.1.5.1.2. **Automated Call Distribution**. USAFE has ten independent Cisco Unified Contact Center Express (UCCX) systems deployed in Europe to support the primary medical centers supporting Airmen and their dependents. These systems are critical to each wing's readiness. These systems support medical, dental, mental health, optometry, and other appointment call trees requiring call agents. Medical appointment lines must be operational during duty hours, and, when down, become a critical outage impacting the wing commander's readiness. Scripting is required for the operation and sustainment of this system.

2.1.5.1.3. **Voicemail.** Cisco Unity Connect is the current voicemail system deployed. Unity voicemail services are available with each call cluster. USAFE-AFAFRICA is licensed to provide 32K mailboxes.

2.1.5.1.4. **Voice Gateway Router (VGR)**. USAFE-AFAFRICA employs VGRs to translate Internet Protocol (IP) to legacy Time Division Multiplexing (TDM) signals (e.g., T1 or E1 interfaces to Defense Switched Network or European commercial service providers, respectively). Each VGR is configured with Cisco Survivable Remote Site Telephony (SRST) to provide a local failover option should the CUCM fail. Each base has a minimum of two Cisco 3945 VGRs, with approximately 50 VGRs across the MAJCOM. Technicians supporting VGRs shall have experience in analog telephony (e.g., primary rate interface, T1/E1, signaling, routing) and IP telephony.

2.1.5.1.5. **Analog Voice Gateway (VG).** VGs provide USAFE-AFAFRICA with an inexpensive means to continue to use analog devices that cannot be transitioned to IP services. The USAFE-AFAFRICA baseline includes various Cisco Voice Gateways. Experience required is equivalent to that of the VGR, and the KTR shall be familiar with legacy TDM endpoints other than telephones (e.g., medical systems alarms).

2.1.5.1.6. **Session Border Controller (SBC)**. SBCs are voice and video firewalls for IP systems. All call clusters configured in the local session controller (LSC) configuration will have an SBC. The KTR shall have advanced CUCM professional level experience and Session Initiation Protocol (SIP) troubleshooting skills to ensure the boundary is properly protected.

2.1.5.1.7. **UC Public Key Infrastructure certificates**: The USAFE-AFAFRICA UC program uses DoD-issued Public Key Infrastructure (PKI) certificates, which require renewal prior to expiration. Updating certificates is time consuming because it requires a formal request process, coordination with AFPKI System Program Office (SPO), and an authorized service interruption (minimum of 45 days advance notice). The following UC devices employ PKI: CUCM, Voice Gateways (VGs), VGRs, SBCs, and Cisco Prime servers.

2.1.5.1.8. **Legacy Voice Transition:** The KTR shall assist units with migrating legacy (e.g., E1, T1) interfaces from legacy equipment to IP infrastructure. USAF legacy telephone switches (e.g., DMS 100) are at end-of-life, with end-of-support expected in 2020-2023. Subsequently, USAFE-AFAFRICA expects to migrate all primary services to the UC infrastructure. Transition work will persist through 2023. A number of legacy UC requirements have approved standard solutions, however, many unique circuits and customer requirements require engineering support to provide solutions. Examples of specialized circuits requiring integration onto the UC platform are: Command Post, Aircraft Landing System support, commercial telephony, Defense System Network, circuits supporting mobile devices, specialized telephony to support flight-line emergencies and Private Branch Exchange connections which support various tenant organizations. Other activities involved with legacy voice migration include: project planning, aggregating IP and telephony data from across the Command, and configuration and installation of UC equipment to support legacy TDM transition.

2.1.5.1.9. **Enhanced 911 (E911).** The Air Force Life Cycle Management Center (AFLCMC) deployed the E911 system across the Air Force. It comes with a sustainment support contract that provides the bases with hardware and application support. The system processes automatic number information from the CUCM through the Cisco VGRs. The KTR shall support CUCM/VGR interface migration, modification, and troubleshooting requirements.

2.1.5.1.10. **Call Detail Record (CDR) and Billing.** Unique Communications' cairs.net product is the IP-based telephone management system used by USAF bases to replace the legacy CAIRS32 system deployed with the Avaya DMS/SL 100 telephone switches. Cairs.net pulls CDR data from the telephone system for organizational billing and E911 location information, and some bases use it to document fiber optic and copper connections. USAFE-AFAFRICA is currently migrating to the USAF enterprise cairs.net system. The KTR shall support CUCM/VGR interface migration, modification, and troubleshooting requirements.

2.1.5.1.11. **Consolidated Operator Answering System (COAS).** Operator assisted calls across the Command are managed by Ramstein AB operators. The transition of the legacy voice system supporting COAS includes servers at each MOB to support COAS applications and IP telephony data transport. Operation and maintenance of servers are outlined in paragraphs listed below.

2.1.5.1.11.1. The KTR shall administer, operate, and maintain the MAJCOM-level COAS servers and server related products and shall provide Tier 2 support, to include software upgrades, patching and vulnerability management.

2.1.5.1.11.2. The KTR shall work with the COAS application maintainers and base level personnel to assist with troubleshooting COAS application related issues.

2.1.5.1.11.3. The KTR shall support future downward-directed systems that mayreplace and/or modify existing systems.

2.1.5.1.12. **Development, Security & Operation (DevSecOps)**. The DevSecOps platform is built on Pivotal Cloud Foundry (PCF) to provide Platform as a Service (PaaS) which is integrated with other technologies. The platform utilizes Hyperconverged technologies along with vSphere and VMWare. USAFE A6 seeks to operate, maintain, and continuously improve the state of the running development environment through automation and the addition of new capabilities.

2.1.5.1.12.1. The KTR shall function as the team leader, platform maintainer, developer and trainer of the USAFE DevSecOps PCF instantiation. As lead the KTR will be responsible for interpreting customer needs, identifying associated Business/Technical Requirements, and advising the Government on scope and schedule parameters to execute projects. The product manager then leads the team in meeting those requirements following industry best practices.

2.1.5.1.12.2. The KTR shall be responsible for the installation, maintenance, upgrades, monitoring, and management of Cloud Foundry as a managed service. Along with managing the entire deployment and operations lifecycle of these platforms, supporting technologies and maintenance of cloud hosted applications.

2.1.5.1.12.3. The KTR shall train airmen, civilian, and KTR personnel in the concepts needed to work with and deploy applications on PCF. The KTR shall train students how to push applications to PCF (various languages), and many of the concepts and features of the PCF platform, including services, log draining, metrics, buildpacks, service brokers, and route services. The KTR shall teach topics directly related to the design and running of cloud native applications.

2.1.5.1.12.4. The KTR shall have knowledge and experience with cloud providers and infrastructure as a service, with 2 to 3 years' experience with a platform as a service product such as Cloud Foundry, Heroku, Elastic Beanstalk, or similar and experience in using Docker, Kubernetes or container orchestration. Experience with Chef, Puppet, BOSH, Terraform or related automation/orchestration tools. The KTR shall have a clear understanding of cloud service and deployment models. The KTR shall have a working knowledge in Java (or equivalent languages), with significant experience with Java Standard Edition (SE) and Java Enterprise Edition (EE). The KTR shall meet the minimum experience requirements of para B.1.1. and Spring Framework experience is desirable.

2.1.5.2. **Network Management System (NMS) Administration**. USAFE-AFAFRICA employs SolarWinds in the SIPRNet and NIPRNet environments.

2.1.5.2.1. The KTR shall administer, operate, and maintain the MAJCOM-level servers and products and shall provide Tier 2 support, to include software upgrades, patching and vulnerability management, to USAFE-AFAFRICA Tier 1 organizations.

2.1.5.2.2. The KTR shall develop and maintain MAJCOM-level standards, maps, and configurations and coordinate implementation of those standards among the Tier 1 organizations. These documents shall be posted IAW para 2.4.5.

2.1.5.2.3. The KTR shall support future downward-directed systems that may replace the existing NMS.

2.1.5.3. **Virtual Desktop Infrastructure (VDI)/SecureView.** (ME services, see para 2.4.2.). The KTR shall provide Tier 2/3 O&M support to include applicable cybersecurity services for USAFE-AFAFRICA's VDI and SecureView environments (currently on SIPRNet only). The KTR shall be responsible for O&M on all servers, storage, applications, and network equipment as identified in Appendix E. O&M services include support for the current SecureView Commercial Solutions for Classified (CSfC), VDI server, and VMware environments. The current USAFE Infrastructure will be used – the KTR does not provide any software. Base level is responsible for Tier 1 support and all user endpoints.

2.1.5.4. **NIPRNet/SIPRNet Microsoft SharePoint and Customer Relationship Management (CRM).** (ME services, see para 2.4.2.). USAFE-AFAFRICA currently operates and maintains SharePoint/CRM environments on NIPR and SIPR supporting 40,000 users globally. The KTR shall administer, operate, and maintain SharePoint/CRM services and provide Tier 2 support to Tier 1 Unit Site Collection Administrators who communicate with users

2.1.5.5. **NIPRNet/SIPRNet Load Balancers.** (ME services, see para 2.4.2.). USAFE-AFAFRICA currently employs F5 Big IP load balancers to provide fault tolerant, load balanced collaboration services throughout the command. The KTR shall administer, operate, and maintain NIPRNet/SIPRNet collaboration, load balancer services.

2.1.5.6. **NIPRNet/SIPRNet Enterprise Structured Query Language (SQL) database.** (ME services, see para 2.4.2.). The KTR shall administer, operate, and maintain enterprise Microsoft (MS) SQL services in support of A6-managed, or A6-approved, systems. Support includes, but is not limited to, the following: database clustering, database management, security, performance analysis, backup and restoration, and Microsoft Windows Server operating system support.

2.1.5.7. **NIPRNet/SIPRNet Tasker Management Tool (TMT).** (ME services, see para 2.4.2.). USAFE-AFAFRICA currently employs Accenture TMT as its automated system of tracking workflow associated with formal taskings. The KTR shall administer, operate, and maintain NIPRNet/SIPRNet Tasker Management Tool services for approximately 3,500 users.

2.1.5.8. **SIPRNet Unified Collaboration Product.** (ME services, see para 2.4.2.). USAFE-AFAFRICA currently employs Microsoft Skype for Business as its unified collaboration product on SIPRNet. The KTR shall administer, operate, and maintain SIPRNet unified collaboration product services for approximately 15,000 users.

2.1.5.9. **Data Center Operation.** (ME services: 2.1.5.9. – 2.1.5.9.2., see para 2.4.2.). The KTR shall operate and maintain the data center production environment with duties to include oversight of VMware and Cisco virtualization technologies, storage management, capacity planning, performance management, systems automation, facility management, asset management, problem management, change management, backup and recovery, archiving, business continuity planning, continuity of operations (COOP) and services failover, availability management, and the integration and co-existence of these technology categories.

2.1.5.9.1. The KTR shall operate and maintain Cisco data center infrastructure. Technology examples include Virtual Extensible Local Area Network (VXLAN), Virtual Storage Area Network (VSAN), Fiber channel, routing and switching protocols.

2.1.5.9.2. The KTR shall ensure the proper functioning of the Data Center COOP capability. The KTR shall, at a minimum, test COOP annually.

2.1.5.10. **Enterprise Virtualization Management (EVM).** (ME services, see para 2.4.2.). Support is focused on a combination of both on-site and remote, proactive support (.e.g. plan, design, develop, test, implement (to include the use of pilots), optimize and integrate with existing and future IT systems. The KTR shall perform such tasks as operating and maintaining a centralized operations environment; engineering and installation (E&I) of virtualization technologies; performance tuning, problem resolution, disaster recovery (DR); data/site replication management, data backup and archiving; incident, problem, and resource reporting; configuration management; product evaluations and implementations, validating and qualifying new solutions and enhancements to existing solutions. Equipment and software currently installed is listed in Appendix E: Hardware and Software. The KTR shall submit work documents such as design plans, implementation plans, and test plans; technical reports; assessments to the COR or TR within the time line specified by the Government representative.

2.1.5.11. The KTR shall oversee daily monitoring of all assigned COOP systems and services to ensure operations are normal. Respond to system outages and assist in team problem triage and remediation of exercise and system outages. Perform activities associated with protection and backup of data to ensure backup processes are successfully completed on a regular basis and provide daily administration, maintenance, installations and upgrades of servers.

**2.2. Systems Engineering & Shared Support.** The KTR shall provide Network and Systems Engineering Support services to improve customer service, security, performance, and reliability for USAFE-AFAFRICA systems and networks.

**2.2.1. Requirements Analysis.** The KTR shall assist the Government in assessing system performance, planning for new and evolving IT systems, evaluating design proposals for the migration of existing functionality, and making recommendations for corrections and enhancements. KTR planning services shall include providing draft documentation and technical input to requirements analysis, design and engineering, test, implementation, and architecture documentation for new, evolving, and existing IT systems. The KTR shall conduct and/or participate in strategic planning, studies, and evaluations to provide resource requirements, present recommended solutions, determine labor and tools estimates, and plan/refine schedules. The KTR shall include the following:

2.2.1.1. Provide technical studies, review plans, evaluate technologies prior to fielding new releases or systems.

2.2.1.2. Review IT plans and policies, and make recommendations for improvement.

2.2.1.3. Research and coordinate technical issues and requirements and draft newand updated policy governing technical issues.

2.2.1.4. Provide technical analyses and draft reports of IT system tests, assessments, and architectures.

2.2.1.5. The KTR shall post these documents within 2 business days of assessment, unless a time extension has been extended to the KTR, in writing, by the COR or TR (RR#: A009 & A037).

**2.2.2. Systems Integration.** As services and technologies evolve, new software and hardware will need to be incorporated into the existing baseline as determined by the applicable Government agent. Also, as threats emerge, new security measures will be developed and require integration into existing baselines. The KTR's effort shall include the following:

2.2.2.1. Test and evaluate commercial-off-the-shelf applications, Government-off-the-shelf applications and hardware for integration into the USAFE-AFAFRICA IT systems and networks.

2.2.2.2. Ensure compatibility with current baseline resolving conflicts as they arise.

2.2.2.3. Apply appropriate security measures (STIGs, Information Assurance Vulnerability Management (IAVMs), Tasking Order Compliance, etc.) to lock down the application/hardware.

2.2.2.4. Develop deployment procedures (e.g., package software, installation instructions). Post documentation and obtain COR or TR approval prior to release (RR#:A010).

2.2.2.5. Coordinate with Cyber Surety prior to deployment. Test and evaluate directed patches for compatibility with the current baseline, and resolve any conflicts prior to deployment.

**2.2.3. Enterprise Network Engineering.** (ME services: 2.2.3. – 2.2.3.14., see para 2.4.2.). The KTR shall provide System Engineering services for complex, large-scale, and/or enterprise-type projects. The KTR shall provide the following services:

2.2.3.1. The KTR shall provide on-site systems architecture, analysis, design and engineering support services for unclassified and classified HQ USAFE-AFAFRICA communications networks with respect to routing and switching; security; voice, video, and collaboration; data center infrastructure; IP quality of service; capacity and continuity planning; performance, problem and change management; and the integration and co-existence of these technology categories.

2.2.3.2. Participate in systems engineering planning activities. Provide feedback to both short-range and long-range planning activities to enhance performance and improve efficiency. Post feedback within 5 business days of planning activities (RR#: A011).

2.2.3.3. Provide emerging communications and IT engineering support and technical solutions to improve overall service delivery to include customer support, network, services, proactive system support, etc.

2.2.3.4. The KTR shall advise HQ USAFE-AFAFRICA/A6 staff on current and planned projects (involving technologies, methodologies, tools, etc.) to improve network optimization. Support may include reviewing design requirements, priorities, and goals, analyzing impacts of new requirements on the existing network, and reviewing network architecture/topology, protocol selection and configuration, feature selections/configurations and security considerations. The KTR shall post required reports/documents within 5 business days of review, unless a time extension has been extended to the KTR, in writing, by the COR or TR (RR#: A012).

2.2.3.5. Develop Cost Benefit Analysis documentation in support of new technology or processes. The KTR shall post documentation within 5 business days of creation or review, unless a time extension has been extended to the KTR, in writing, by the COR or TR (RR#: A013).

2.2.3.6. Provide design and engineering support for new network and system implementations and upgrades to include hardware, software, projection systems, video switching hardware, video teleconferencing, and other systems to meet project requirements.

2.2.3.7. The KTR shall provide technical solutions to complex problems to include Tier 3 troubleshooting of O&M problems.

2.2.3.8. The KTR shall troubleshoot network hardware, software, firmware and configuration issues, and document findings and post Network Health Assessment Report within 3 business days of completion (SS#: 5; RR#: A005).

2.2.3.9. The KTR shall provide network change support for hardware, software, firmware or configuration events that may involve evaluating the potential impact of proposed change requests, implementation procedures, technical solutions, project plans and project support agreements. The KTR shall post a Network Change Impact Report within 10 business days of notification (RR#: A014).

2.2.3.10. The KTR shall implement and integrate technical requirements and design goals into the overall network design. The KTR shall prepare project implementation documentation to include requirements documents, technical solutions, project plans, project support agreements, and change requests. The KTR shall post required reports/documents within 5 business days of notification (RR#: A015 & A038).

2.2.3.11. The KTR shall provide performance engineering and optimization analysis to sustain a high-performance network and meet the changing demands on the network. The KTR shall provide analysis of network configurations against industry best practices. The KTR shall post a Performance Engineering and Optimization Report within 45 business days of notification (RR#: A016).

2.2.3.12. The KTR shall provide a Network Health Assessment Report on each of the 6 MOB's,. and one GSU as directed, NIPRNet and SIPRNet Infrastructures annually. Individual base report and a consolidated summary report shall be posted (IAW para 2.4.5) not later than (NLT) the 180th calendar day, or next business day of the year's identified period of performance (SS#5; RR#:A005).

2.2.3.13. The KTR shall provide training and guidance on internetworking product and technology topics. This may include posting white papers , design guides, case studies, configuration guides, troubleshooting guides, deployment guides and training documents within 5 business days of notification (RR#: A062).

2.2.3.14. The KTR shall attend, conduct and participate in meetings, teleconferences, briefings, and conferences approved by the COR/TR and Contracting Officer (CO); and post a written summary (meeting minutes) of key information, actions and contacts within 5 business days of the event (RR#: A017).

2.2.3.15. The KTR shall manage the USAFE-AFAFRICA enterprise network management solution. The network management solution will be provided by A6 and consist of network performance module, netflow collector and analyzer module, network configuration manager, network mapping, and IP address management (IPAM) module. Both NIPRNet and SIPRNet network managements systems will manage and monitor respective networks. The KTR shall post a baseline for each network management system (NMS) configuration for approval, within 2 business days of creation/update (RR#: A027). The KTR shall implement the approved baseline for all sites using the NMS.

2.2.3.16. The KTR shall provide on-site systems architecture, analysis, design and engineering support services for Multiprotocol Label Switching (MPLS) networks. The KTR shall configure and troubleshoot MPLS on network hardware.

2.2.3.17. The KTR shall provide on-site systems architecture, analysis, design and engineering support services for unclassified and classified HQ USAFE-AFAFRICA data centers and data center COOP. The KTR shall provide and ensure implementation of best practices required to design, implement, and manage data center infrastructure and troubleshoot as required.

2.2.3.18. The KTR shall provide on-site systems O&M and engineering support services for HQ USAFE-AFAFRICA CSfC communications networks with respect to routing, switching, and security. The O&M functions include but are not limited to Virtual Private Network (VPN) gateways, Intrusion Protection Systems, Firewalls, and network infrastructure devices.

**2.2.4. Technical Project Management (PM) Support:** The KTR shall provide centralized project management support to integrate, monitor and control interdependencies among USAFE-AFAFRICA projects. Depending upon the scope, size, complexity, and Government needs, the KTR will be a member of an integrated project management team consisting of both Government and other KTRs. The project charter shall clearly identify the ITSS-II KTR's roles and responsibilities for the particular project.

2.2.4.1. The KTR shall ensure that activities and processes are coordinated and integrated in accordance with A6's documented processes (when they exist) or sound Project Management Institute (PMI) framework (when they don't). As needed, these processes include applying an integrated, standards-based project management approach lifecycle to accomplish the following:

2.2.4.2. The KTR shall balance competing constraints of scope, quality, schedule, budget, resources, and risk while satisfying project requirements and addressing stakeholder expectations.

2.2.4.3. The KTR shall define and manage project management processes, project schedule, quality standards, measures and metrics, configuration management; change management, and risks and issues. The KTR shall post the documentation within 5 business days of creation or review, unless a time extension has been extended to the KTR, in writing, by the COR or TR (RR#: A018).

2.2.4.4. Specific project management support to lead the planning and implementationof projects shall include the following:

2.2.4.5. Facilitate the definition of project scope, goals, and required reports/documents through interaction with the stakeholders/customers in requirements gathering meetings.

2.2.4.6. Develop project charter, scope document, and requirements specification as need to satisfy project needs. The KTR shall post the documentation within 5 business days of creation or review, unless a time extension has been extended to the KTR, in writing, by the COR or TR (RR#: A018).

2.2.4.7. Develop a project plan, for COR or TR review and approval, that defines, at a minimum, the scope, goals, required reports/documents, schedule/milestones, resource requirements, and work breakdown structure (WBS). The KTR shall post the documentation within 5 business days of notification of the requirement by the COR or TR, unless a time extension has been extended to the KTR, in writing, by the COR or TR (RR#: A039).

2.2.4.8. Manage the project, tracking project required reports/documents and materials to facilitatecompletion of the work on time and within the established budget.

2.2.4.9. Reporting status to stakeholders within 5 business days of notification of the requirement by the COR or TR, unless a time extension has been extended to the KTR, in writing, by the COR or TR.

**2.2.5. Cybersecurity Services:** (ME) services: 2.2.5. – 2.2.5.8.8., see para 2.4.2.) The KTR shall implement cybersecurity strategies for the USAFE-AFAFRICA networks consistent with USAF, DoD, and National Security Agency (NSA) guidance. The KTR shall provide services and support to ensure the confidentially, integrity and availability of USAFE-AFAFRICA accredited Command, Control, Communications and Computer (C4) networks. USAFE-AFAFRICA require all C4 networks be protected from network attacks, unauthorized access, service interruption and unauthorized disclosure or modification of information. The KTR shall research, develop and implement a holistic risk management strategy for C4 networks to enable the execution of USAFE-AFAFRICA operations. Cybersecurity is highly regulated, and strict adherence to USAF and DoD directives and USAFE-AFAFRICA policies and procedures is required. The KTR shall provide the following Cybersecurity Services:

2.2.5.1. Manage A&A for communications and information systems under A6 purview.

2.2.5.1.1. Develop and maintain A&A documentation for A6-managed SIPRNet and NIPRNet systems. This includes, but is not limited to, Risk Management Framework (RMF)/DoD Information Assurance Certification and Accreditation Process packages, network diagrams, IP ranges, COOP, disaster recovery plans (DRP), configuration management plans, vulnerability management plans, and systems plans of action and milestones (POA&M). The KTR shall post the documentation within 5 business days of creation or review, unless a time extension has been extended to the KTR, in writing, by the COR or TR (RR#: A019).

2.2.5.1.2. Perform on-site A&A assessments (e.g., Information Assurance (IA) Control Validation) on A6-managed systems.

2.2.5.1.3. Ensure A&A documentation is populated and maintained in the appropriate SIPRNet or NIPRNet Enterprise Mission Assurance Support System (eMASS).

2.2.5.2. Prepare for, assist with, and monitor cybersecurity assessments (networkreadiness assessments, DISA Security Readiness Reviews, Command Cyber Readiness Inspections, National Security Agency (NSA) Red and Blue Team assessments, vulnerability scans, A&A reviews for A6. Develop and/or implement corrective courses of action for findings identified during assessments. Resolve open security vulnerabilities, focusing on the most critical vulnerabilities first.

2.2.5.3. Ensure all ITSS-II KTR personnel granted privileges elevated or performing cybersecurity functions on USAFE-AFAFRICA systems/networks are trained and certifiedin accordance with DoD Manual 8570.01M, *Information Assurance Workforce Improvement Program*.

2.2.5.4. Integrate cybersecurity principles early in the requirements analysis and designand development phases.

2.2.5.5. Develop technical standards (standard operating procedures; tactics, techniques, and procedures; technical implementation instructions; or other required documentation) for security devices, security operations and other operations as required for Government approval. Ensure all technical standards are updated, maintained, and posted within 3 business days of any creation or update, to ensure a central location for distribution as needed (RR#: A020).

2.2.5.6. Review and, with Government approval, provide input to internal andexternal cybersecurity taskings.

2.2.5.7. Cybersecurity Compliance. The KTR shall provide the following services forA6:

2.2.5.7.1. Support and ensure A6-managed systems are compliant with the DoD IAVM Program.

2.2.5.7.2. Report IAVM compliancy; track Cyber Command (CYBERCOM) Command Tasking Orders (CTOs), fragmentary orders (FRAGO), Information Conditions (INFOCON), Coordinated Alert Messages (CAMs), and other directives for USAFE-AFAFRICA. Perform analysis, implement, and report the compliancy of INFOCON changes and CTO. Post within 5 business days of review (RR#: A051).

2.2.5.7.3. Coordinate vulnerability scans/checks as needed and ensure periodic audits are done using DoD approved vulnerability scan tools. Evaluate and ensure security threats are mitigated, remediated or waived in accordance with accepted time constraints.

2.2.5.7.4. Comply with DoD ports and protocol management program. Track and document approved “opened” ports and protocols inbound and outbound. Post results/updates within 5 business days of review (RR#: A052).

2.2.5.7.5. Document and maintain an approved software and hardware baseline for all IT systems under the purview of USAFE-AFAFRICA. This includes, but is not limited to, routers, switches, servers, workstations, etc. Post within 5 business days of review (SS#: 5; RR#: A002).

2.2.5.7.6. Conduct security engineering reviews and recommendations for increased protection on all A6-managed systems. Includes, but is not limited to new and existing projects, capabilities, configurations, testing, and accredited or proposed systems. Post the review results within 2 business days of completion (RR#: A021).

2.2.5.7.7. Define requirements or objectives and recommend solutions for an acceptable level of accreditation for the authorizing official. Post within 5 business days of completion (RR#: A022).

2.2.5.7.8. Provide technical security reviews and recommendations on all software and hardware. Includes, but is not limited to, information assurance tools, network tools, existing baseline software builds, and new proposed solutions across the enterprise. Post within 5 business days of completion (RR#: A023).

2.2.5.7.9. Provide security reviews and recommendations to enhance the security posture on all existing and proposed enterprise network configurations within the accreditation boundary; this also includes approved tunnels and remote connections. Post within 5 business days of completion (RR#: A023).

2.2.5.7.10. Ensure the network architecture plan is documented and an acceptable risk decision is provided to the authorizing official on the existing and changed configurations. Post within 5 business days of completion (RR#: A040).

2.2.5.7.11. Review and implement STIGchecklist required for all A6 managed systems and all A6 implemented systems; the KTR shall provide electronic copies of completed checklist to responsible A&A package owner before system transfer or project closeout. Post completed/updated checklist within 5 business days of completion and include the COR and TR in the email distribution process (RR#:A024).

2.2.5.8. Develop Defensive Cyberspace Operations (DCO) Capabilities.

2.2.5.8.1. Establish and operate a DCO Cell that plans, coordinates, and tracks DCO Response Actions and Internal Defensive Measures, as defined in Joint Publication 3-12(R) *Cyberspace Operations*, Chapter 2.a (2), in steady state and crisis action environments in reaction to all applicable indications, warnings, threats, and attacks.

2.2.5.8.2. Refine and complete development of USAFE-AFAFRICA DCO Concept of Operations (CONOPS) for Government approval. CONOPS will provide the mechanism to gain visibility of enterprise-wide assets and operations, integrate intelligence monitoring information, implement higher headquarters (HHQ) governance, and align Air Force weapon systems and applicable support systems programs to a common model based on lessons learned and best practices from available resources. Post CONOPS within 30 business days of tasking by the COR or TR. (RR#: A047).

2.2.5.8.2.1. Perform annual reviews of the DCO CONOPS and coordinate approval of changes.

2.2.5.8.2.2. Develop, for Government approval, methods to implement DCO CONOPS responsibilities, plans, documentation, and sustainment requirements. Once approved, maintain and coordinate methods among the implementing organizations. Ensure all methods are updated, maintained, and posted within 3 business days of any creation or update, to ensure a central location for distribution as needed (RR#: A020).

2.2.5.8.2.3. Develop methods to gather and document requirements to support the design, implementation, and operation of the tools, processes, and procedures of the DCO CONOPS. Ensure all methods are updated, maintained, and posted within 3 business days of any creation or update, to ensure a central location for distribution as needed (RR#: A020).

2.2.5.8.3. Monitor subordinate USAFE-AFAFRICA communication units to ensure they comply with USCYBERCOM, AFCYBER directions and tasking and operational orders (TASKORDS/OPORDS). Notify the Government COR or TR of any non-compliance.

2.2.5.8.4. Develop, for Government approval, USAFE-AFAFRICA DCO Cell documentation to include instructions directing command and control processes that clarify the relationships among Mission Defense Teams (MDT), cyber security requirements, and DCO Response Actions and Internal Defensive Measures. Once approved, coordinate implementation among implementing organizations. Ensure all documents are updated, maintained, and posted within 3 business days of any creation or update, to ensure a central location for distribution as needed (RR#: A020).

2.2.5.8.5. Develop and maintain a collaborative environment that provides mechanisms to coordinate, disseminate, and track DCO planning and execution actions.

2.2.5.8.6. Develop DCO-focused measures, tactics, techniques, and procedures for weapon and associated support systems within the USAFE-AFAFRICA area of operations as required for Government approval. Ensure all tactics, techniques, and procedures are updated, maintained, and posted within 3 business days of any creation or update, to ensure a central location for distribution as needed (RR#: A020).

2.2.5.8.7. Document standards for USAFE-AFAFRICA DCO forces interim operational capability (IOC) and full operational capability (FOC) in line with applicable USCYBERCOM, Headquarter Air Force (HAF)/Secretary of the Air Force (SAF), and AFCYBER directions and TASKORDS as required for Government approval. Ensure all standards are updated, maintained, and posted within 3 business days of any creation or update, to ensure a central location for distribution as needed (RR#: A020).

2.2.5.8.8. Develop enterprise views of MDT readiness IOC and FOC criteria and procedures to manually or automatically update this view. Ensure all views are updated, maintained, and posted within 3 business days of any creation or update, to ensure a central location for distribution as needed (RR#: A020).

**2.2.6. Architecture Support**. The KTR shall provide the following support and services:

2.2.6.1. Develop, document, and maintain the high-level architecture for USAFE-AFAFRICA MAJCOM-unique systems and networks.

2.2.6.2. Ensure the high-level architecture complies with A6 goals and objectives and AF and DoD policy and initiatives (e.g., Joint Information Environment, Data Center Optimization Initiative).

2.2.6.3. Attend, conduct, and participate in taskers, briefings, meetings, teleconferences, and conferences with DoD organizations (COCOMs, SAF) relating to high-level architecture for USAFE-AFAFRICA systems and networks, when directed by the Government representative.

**2.2.7. Configuration Management.** The KTR shall provide configuration management of the A6-managed networks and systems. The KTR shall implement and maintain a configuration management program that encompasses documented change control procedures and practices for both hardware and software on all supported networks/systems. The KTR shall document all procedures/practices in a configuration management plan, which shall be posted for Government approval within 2 business days of completion (RR#: A041).

2.2.7.1. The program shall complement and work in concert with A6 Change Control Board (CCB) activities. The scope of this work shall include the following:

2.2.7.1.1. Support the activities of the A6 CCB.

2.2.7.1.2. Record and post CCB minutes and supporting documents (e.g., action items) within 5 business days of event. (RR#: A017).

2.2.7.1.3. Establish, maintain and post within 2 business days, upon creation or update, configuration data for supported IT systems including, but not limited to, type and serial number, maintenance history, warranty information, and license information (RR#: A053).

2.2.7.2. Ensure proper licensing for software in use on supported systems and networks. Maintain a system of licensing accountability and internal control procedures and post within 90 business days performance start or 5 business days of review/update (SS#: 5; RR#: A006).

2.2.7.3. Maintain the license, warranty, and support services data for hardware and software. The KTR shall track periods of performance, notify the Government of expiration 1 year prior to the year of expiration, document and post updates of the periods of performance in the technology roadmap within 2 business days of review/update (SS#: 5; RR#: A006).

2.2.7.4. Make recommendations for communications and IT system improvements that result in optimal hardware and software usage. The recommendations shall be posted within 2 business days of review completion (RR#: A054).

2.2.7.5. Maintain documentation on the configuration of the network and its components to include network architecture diagrams. Post the documentation within 2 business days of completion (RP#: A055).

2.2.7.6. Document all changes to the configuration of the network. Post the documentation within 2 business days of completion (RR#: A056)

2.2.7.7. Document current revision level of all key network components. Post the documentation within 2 business days of completion. (SS#: 5; RR#: A057).

2.2.7.8. Maintain all required documentation relating to domain name service, IP addressing, and host naming. Post the documentation within 2 business days of completion (RR#: A058).

2.2.7.9. Create and maintain inventory of all data center, server, and network assets. Post the initial documentation within 90 business days of performance start and post updates within 5 business days of any change to the inventory. (SS#: 5; RR#: A007).

**2.2.8. Mission Relevant Terrain-Cyber/Mission Mapping (MRT-C/MM).** (ME services: 2.2.8. – 2.2.8.1.7., see para 2.4.2.). MRT-C/MM is one of USAFE-AFAFRICA's top priorities, and relevant objectives of this PWS include characterization and documentation of existing and future data centers and network infrastructure and systems analysis to determine IT system dependencies and vulnerabilities. MRT-C/MM is a broad and comprehensive effort to identify key mission capabilities across the MAJCOM and map those key capabilities to supporting communications systems and infrastructure. MRT-C/MM supports AF Critical Asset Risk Management (CARM) by establishing criticality of infrastructure and assets tied to impact on missions. The initial and primary focus of MRT-C/MM will be on USAFE-AFAFRICA NIPRNet and SIPRNet infrastructures; the scope could expand to other networks with equal or higher classifications. As USAFE-AFAFRICA further consolidates its communications infrastructure (e.g., Data Center Optimization Initiative [DCOI], and European Infrastructure Consolidation [EIC] efforts), it must do so with minimal impact to key mission capabilities.

2.2.8.1. **Systems Analysis**. The KTR shall assist A6 with required systems analysis support to analyze USAFE-AFAFRICA IT environments, supported by network characterization and documentation tasks in this PWS, to determine IT system dependencies and vulnerabilities. The initial and primary focus of MRT-C/MM will be on USAFE-AFAFRICA NIPRNet and SIPRNet infrastructures; however, the scope could expand to other networks with equal or higher classifications. As USAFE-AFAFRICA further consolidates its communications infrastructure (e.g., data center consolidation, and European infrastructure consolidation efforts), it must do so with minimal impact to key mission capabilities. While the KTR will not be responsible for identifying or prioritizing key mission capabilities, the KTR shall work with other government and KTR personnel, as part of integrated product teams (IPT) or operational planning teams (OPT), to identify supporting communications and infrastructure and map those supporting capabilities to key missions identified by the IPT/OPT. The KTR shall assist in the identification, assessment, analysis, and management of Task Critical Asset (TCA) related cyber issues supporting CARM and participate in the Mission Assurance Assessments (MAA) as required by theGovernment representative. Post the documentation within 5 business days of creation or review, unless a time extension has been extended to the KTR, in writing, by the COR or TR (RR#: A025).

2.2.8.1.1. The KTR shall become familiar with the Functional Mission Analysis (FMA) process. FMA is an application of operational design principles, which helps leaders understand (and modify) mission specific dependencies. It is also a problem framing methodology to help cope with the complexity of mission mapping. The KTR shall follow the FMA process: understand supported mission and guidance, establish mission purpose and goals, establish unacceptable losses, establish hazardous system states, build mission model, create mission functional control structure, analyze model, identify critical info flows and associated hazards, and generate causal scenarios. The KTR will not be responsible for identifying or prioritizing key mission capabilities.

2.2.8.1.2. The KTR shall attend, at Government expense, the USAF FMA training if it becomes available after the period of performance start date.

2.2.8.1.3. The KTR shall participate in small, Government led innovation teams or IPTs to develop solution proposals for USAFE-AFAFRICA based on A6 technical and business requirements, and provide subject matter expertise in support of A6 initiatives. The KTR shall post resulting engineering/ implementation plans within 3 business days of notification of the requirement by the COR or TR, unless a time extension has been extended to the KTR, in writing, by the COR or TR (RR#: A042).

2.2.8.1.4. The KTR shall take part in OPT meetings for ongoing and future contingency operations. The KTR shall review, edit, or create documents required to highlight communications and IT impacts with A6 equities. The KTR shall identify single points of failure and designs for corrective actions, and post results within 2 business days when the task has been completed (RR#: A043).

2.2.8.1.5. The KTR shall create an IT technology roadmap, based on A6 guidance and direction, and plan and coordinate activities that adhere to the approved A6 roadmap. The KTR shall be responsible for the systems analysis activities and translating customer and organizational goals and objectives into actionable business, organizational, and technology strategies. The KTR shall evaluate and review plans, requirements, technical solutions, and the existing IT landscape to identify inconsistencies with the Government provided technology roadmap. The IT technology roadmap shall be posted within 5 business days of creation or update. (SS#: 5, RR#: A003).

2.2.8.1.6. The KTR shall formulate contingency plans to address schedule revisions, manpower adjustments, and work package requirements. The plans shall be posted within 5 business days of creation or review, unless a time extension has been extended to the KTR , in writing, by the COR or TR (RR#: A044). The KTR shall respond to system failures and work with others to resolve issues related to hardware and software. The KTR shall monitor system resource usage and ensure adequate system resources are available to meet the IT requirements through resource scheduling. The KTR shall notify the COR or TR via e-mail, when resource utilization exceeds published thresholds and no additional resources are available.

2.2.8.1.7. The KTR shall edit, modify, or create “reference and solutions architectures” to the IT design roadmap and post the document within the first 60 days of the first period of performance (RR#: A026).

**2.3. IT/Communications Planning Support**. USAFE-AFAFRICA has a requirement to provide IT/ Communications planning support onsite at Ramstein AB, DE; RAF Lakenheath, UK; RAF Croughton, UK; Spangdahlem AB, DE; Aviano AB, IT; and Incirlik AB, TR. The KTR shall provide the following services:

**2.3.1. Plans, Process, and Policy Support.** The KTR shall analyze HQ USAFE/AFAFRICA, and/or assigned bases IT/Communication strategic level guidance, such as program action directives, program guidance letters, programming plans, wing plans, or reference architectures to develop planning documents, transition strategies, and policies in order to meet and implement base, A6, Joint Information Environment, DoD-Chief Information Officer (CIO), and Secretary of the Air Force (SAF)-CIO program objectives. The KTR shall exhibit extensive telecommunication background and experience by supporting the communication squadron staff in developing a future roadmap or architecture and associated CONOPS. The KTR shall post proposed solutions within 5 business days of creation or update, unless a time extension has been extended to the KTR, in writing, by the COR or TR (SS#: 5; RR#: A004). The objective is to determine a clear vision and concept for the future and recommend, to the Government, path to take in order to transform these visions into reality. Required tasks follow:

2.3.1.1. Analyze communications/IT requirements to determine validity, accuracy, or feasibility for implementation. Resolve discrepancies with appropriate agencies in order to meet objectives. Unresolved discrepancies shall be posted not later than (NLT) later than 2 business days after discovery (RR#: A048).

2.3.1.2. Research and document proposed infrastructure and system topologies including architecture, system connectivity, and interoperability. Documents shall comply with AFI 17-140, *Air Force Architecting*, and the KTR shall post documents within 10 business days of creation or review, or notification of requirement by the COR or TR (RR#: A028).

2.3.1.3. Recommend standards, procedures, and enhancements for implementation and maintenance of new technologies. The KTR shall post recommendations within 10 business days of creation or review, or notification of requirement by the COR or TR (RR#: A029).

2.3.1.4. Review and coordinate on the technical content of design proposals presented by KTR, USAF or DoD engineers for the construction or renovation of facilities, technical quality of equipment to be installed, installation of equipment, and maintenance of equipment. Provide expert advice on equipment specifications, capabilities and operational procedures, providing guidance for selection and acquisition of Command, Control, Communications, Computer and Intelligence (C4I) equipment and infrastructure. The KTR shall post comments and recommendations within 10 business days of review, or notification of requirement by the COR or TR (RR#: A030).

2.3.1.5. Draft segments of planning, transition, and policy documents using applicable directives such as AFI 32-1023, *Designing and Constructing Military Construction Projects* and AFI 17-140 and industry best practices, such as IT Service Management (ITSM) processes within the Information Technology Infrastructure Library (ITIL v3) framework, following DoD and Air Force policy and guidance. The KTR shall post documents within 15 business days of creation, or notification of requirement by the COR or TR (RR#: A031).

**2.3.2. Project Management Support.** The KTR shall perform project management tasks in accordance with Methods and Procedures for Technical Orders (MPTO) 00-33A-1001, *General Cyberspace Support Activities Management Procedures and Practice* (Chapters 19 & 20) to support implementation and sustainment of project-related technologies and strategic plans. The KTR shall develop project implementation plans and, after approval from the COR, lead such projects from inception through the completion/sustainment. Required tasks follow:

2.3.2.1. Develop project implementation plans IAW MPTO 00-33A-1001 (Chapter 19) for all approved and funded strategic plans, and interface with appropriate staff and outside agencies to execute those plans. The KTR shall post plans within 10 business days of creation, review, or notification of requirement by the COR or TR (RR#: A045).

2.3.2.2. In developing implementation plans, the KTR shall compare current capabilities with requirements in order to address shortfalls, areas for future concentration, and total cost of ownership.

2.3.2.3. Provide estimates for planning, programming, and budgeting for infrastructure upgrades and/or equipment purchase requirements. The KTR shall post estimates within 3 business days of creation, or notification of requirement by the COR or TR(RR#: A032).

2.3.2.4. Ensure communications systems architecture, configuration, and integration conformity by coordinating engineering data through the Cyberspace Systems Integrator-Base Level.

2.3.2.5. Manage implementation of communication systems projects IAW MPTO 00-33A-1001 (Chapter 19).

2.3.2.6. Facilitate planning meetings, video- and teleconferences. Post meeting minutes within 5 business days (RR#: A017).

2.3.2.7. Coordinate site surveys with internal and external agencies. Prepare site survey results and present briefings, as required. Site survey results shall be posted within 5 business days upon site survey completion (RR#: A059).

2.3.2.8. Coordinate the allocation and/or placement of resources, prepare/review equipment and facility specifications, monitor/resolve technical communication problems and/or conduct operational acceptance in accordance with AFI 32-1023, AFI 17-140, Air Force Engineering Technical Letter (ETL) 02-12, *Communications and Information System Criteria for Air Force Facilities* and other applicable directives. Post resulting documents within 2 business days of completion, or notification of requirement by the COR or TR (RR#: A033).

2.3.2.9. Create, gather and report on metrics for all systems with open projects. The KTR shall post metrics within 2 business days of completion, or notification of requirement by the COR or TR (RR#: A060).

2.3.2.10. Conduct weekly project meetings for all open projects. The KTR shall post meeting minutes within 5 business days of meeting (RR#: A017).

**2.3.3. IT/Comm planning support certifications and experience.**

2.3.3.1. KTR shall ensure KTR personnel possess a Project Management Professional certification, issued by the Project Management Institute (PMI).

2.3.3.2. KTR shall ensure KTR personnel have experience in the following:

2.3.3.2.1. Data Center Architecture.

2.3.3.2.2. Cloud-Based Computing & Services.

2.3.3.2.3. Technical writing.

2.3.3.2.4. System Developmental Lifecycle (SDLC).

2.3.3.2.5. Developing SDLC life cycle management plans.

2.3.3.2.6. Military communication planning (Ref: Air Force MPTO00-33A-1001, Chapters 19 and 20).

2.3.3.2.7. The development of Statements of Work (SOW) and Statements of Objectives (SOO).

**2.4. Other Requirements.**

**2.4.1. Reports/Activity Tracking/Documentation.** The KTR shall keep the COR, or the TR, informed of all activities, as outlined in this PWS, via written e-mail communication. The KTR shall provide reports by electronic means, templates are be provided by the Government via a Share Point site. If the KTR encounters any obstacle in meeting the set delivery deadlines, coordination with the COR or TR, should a new suspense date be required. The KTR shall participate in, and use, government processes and procedures and provided data repositories to track incident, problem, project, task and administrative activities/information. With COR approval, information captured by these means may be summarized and/or referenced rather than duplicated in other reports. For further delivery guidelines see para 2.4.5. The following pre-defined reports are required.

2.4.1.1. **Trip Reports.** The KTR shall post trip reports within 5 business days of the conclusion of travel (RR#: A066). Trip Reports shall contain such information as the dates, locations, purpose and travelers involved in any travel taken in the performance of this task order (TO). The trip report shall identify any issues or risks revealed that may have an impact on the systems and/or programs germane to this TO plus any action item that must be accomplished by any party in order to accomplish the goals of this TO.

2.4.1.2. **Operational and Service Management Reports**. The KTR shall submit work documents such as design, plans, technical reports, assessments, project plans, and other products, as approved, and post within 5 business days of creation, review, or update, unless a time extension has been extended to the KTR, in writing, by the COR or TR (RR#: A061).

2.4.1.3. **Monthly Summary Reports (MSR).** The MSR shall be posted within 5 business days of the beginning of the following month (RR#: A067).

2.4.1.4. **Phase-in Plan**. The KTRs approach to the mobilization period. The plan shall provide detailed descriptions of the steps and responsibilities during the transition phase along with associated timelines (to include start and end dates) and interface with the Government. The plan shall be posted within 2 business days of contract award (RR#: A046). In addition to guiding the phase-in process, the final plan; with descriptive information, problems and solutions; shall be posted within 5 business days of performance start (RR#: A046).

2.4.1.5. All other required reports/documents shall be posted according to the Services Summary (Table 2), unless a time extension has been extended to the KTR, in writing, by the COR orTR.

**2.4.2. Mission Essential (ME).** The overall services detailed in this TO are non-mission essential and non-deployable. The specific services requiring mission essential support during crisis are identified below.

2.4.2.1. Unified Communications: 2.1.5.1. – 2.1.5.1.11.3.

2.4.2.2. VDI/Secure View: 2.1.5.3.

2.4.2.3. NIPR/SIPR MS SP + CRM: 2.1.5.4.

2.4.2.4. NIPR/SIPR Load Balancer: 2.1.5.5.

2.4.2.5. NIPR/SIPR SQL Database: 2.1.5.6.

2.4.2.6. NIPR/SIPR TMT: 2.1.5.7.

2.4.2.7. SIPR Unified Collaboration: 2.1.5.8.

2.4.2.8. Data Center Operations: 2.1.5.9. – 2.1.5.9.2.

2.4.2.9. EVM: 2.1.5.10.

2.4.2.10. Enterprise Network Engineering: 2.2.3. – 2.2.3.14.

2.4.2.11. Cyber Security Services: 2.2.5. – 2.2.5.8.8.

2.4.2.12. MRT-C/MM: 2.2.8. – 2.2.8.1.7.

2.4.2.13. The mission essential support specified above is limited to the standard Place of Performance (see para 4.1.) and all contract employees supporting this TO shall be non-deployable.

**2.4.3. Clearance Requirements.** All KTR personnel working directly on this TO shall possess, at minimum, a United States (U.S.) Secret clearance, except for performance on the DCO requirements of this PWS in paragraph 2.2.5.8. The DCO requirements of this PWS (para 2.2.5.8.) require a Top Secret clearance, due to the systems the KTR will require access to, during the stated support requirements.

**2.4.4. Data Calls.** To collect existing records to complete this task, data calls shall be requested through official forms of communication through government representatives. The primary tool used for requesting information shall be the USAFE-AFAFRICA TMT or electronic Staff Summary Sheet (eSSS).

2.4.4.1. The KTR shall draft TMT or eSSS documents for COR or TR release approval, post within 2 business days of creation. The KTR shall ensure that the TMT task or eSSS is accurate and written in the prescribed format (RR#: A034).

2.4.4.2. The KTR shall collect all data call products processed during performance of this task order and post in the Government provided NIPRNet or SIPRNet document library within 2 business days of any update (RR#: A035).

**2.4.5. Documentation Library:** The KTR shall establish a working and published document library using one of the existing platform utilized by the Government, i.e. Microsoft SharePoint, server or cloud storage. This library will be the official repository for all required reports/documents under this contract.

2.4.5.1. Any time this PWS refers to the term “post or posted” the storage location will be in the applicable project folder in the document library. Unless otherwise defined in this PWS, E-mail notification of the upload (including the link) to the Contracting Officer Representative (COR) or the technical representative (TR) will be considered as compliant with the delivery requirements.

2.4.5.2. KTR shall maintain the record library for the duration of the contract and manage permissions for all who require access within the USAFE-AFAFRICA theater. The COR and applicable Government TR’s will have access.

## 3.0. SERVICES SUMMARY.

**3.1. The Service Summary (SS)**. Will be IAW AFI 63-138, *Acquisition of Services* and Federal Acquisition Regulation (FAR) Subpart 37.6. *Performance Based Acquisition*. SSs defined in this TO.

**3.2. Assessment Method:** Each SS will be assessed and rated on the monthly Quality Assurance Surveillance Plan (QASP) Checklist.

## Table 2. SERVICES SUMMARY (SS).

| SS # | Performance Objective | PWS Para | Performance Threshold |
|---|---|---|---|
| 1 | Engineering and Technical Support | 2. – 2.4.5.2. | Will be delivered on time with no more than one late delivery in the period of performance. No more than one revision per specified delivery/review. |
| 2 | Knowledge Transfer and Mentoring | 2.2.3.13. | Will be delivered on time with no more than one late delivery in the period of performance. No more than one revision per specified delivery/review. |
| 3 | Incident/ Problem Resolution | 2.1.1./ 2.1.1.1./ 2.1.1.3./ 2.1.1.5./ 2.1.5.1.2./ 2.1.1.7./ 2.1.2.1./ 2.1.2.10./ 2.3.1.1. | The KTR shall respond within one (1) hour of an incident ticket being opened and shall be one site within two (2) hours to restore service outages. 95% of all responses are accomplished on time; 5% within four (4) hours. Problem resolutions will be delivered on time with no more than one late delivery in the period of performance. No more than one revision per specified delivery/review. ASI are submitted and approved prior to any upgrade or modification, no deviations from standard. |
| 4 | ASI | 2.1.1.3. | 45 business days prior to any upgrade or modification, 100% of the time. ASI are submitted and approved 45 business days prior to any upgrade or modification, no deviation from standard. |
| 5 | Provides requested/ required documentation, plans, reviews, solutions, reports, & presentation, etc. and materials on time and accurately | 2.1.1.1./ 2.1.2.9./ 2.1.2.13/ 2.1.4./ 2.1.4.3./ 2.2.1.5./ 2.2.2.4./ 2.2.3.2./ 2.2.3.4./ 2.2.3.5./ 2.2.3.8./ 2.2.3.9./ 2.2.3.10./ 2.2.3.11./ 2.2.3.12./ 2.2.3.1.4./ 2.2.3.15./2.2.4.3./ 2.2.4.6./ 2.2.4.7./2.2.5.1.1./ 2.2.5.5./ 2.2.5.7.2./ 2.2.5.7.4./ 2.2.5.7.5./ 2.2.5.7.6./ 2.2.5.7.7./ 2.2.5.7.8./ 2.2.5.7.9./ 2.2.5.7.10./ 2.2.5.7.11./ 2.2.5.8.2./ 2.2.5.8.2./ 2.2.5.8.2.3./ 2.2.5.8.4./ 2.2.5.8.6./ 2.2.5.8.7./ 2.2.5.8.8./2.2.7./ 2.2.7.1.2./ 2.2.7.1.3./ 2.2.7.2./ 2.2.7.3./ 2.2.7.4./ 2.2.7.5./ 2.2.7.6./ 2.2.7.7./ 2.2.7.8./ 2.2.7.9./2.2.8.1./ 2.2.8.1.3./ 2.2.8.1.4./ 2.2.8.1.5./ 2.2.8.1.6./ 2.2.8.1.7./ 2.3.1./ 2.3.1.1./ 2.3.1.2./ 2.3.1.3./2.3.1.4./2.3.1.5./ 2.3.2.1./ 2.3.2.3./ 2.3.2.6./ 2.3.2.7./2.3.2.8./ 2.3.2.9./ 2.3.2.10./ 2.4.2.1.1./ 2.4.1.2./ 2.4.1.3./ 2.4.1.4./ 2.4.4.1./ 2.4.4.2./ 4.3.4./ 4.3.6./ 4.3.7./ 4.4.3./ 4.5./ 4.7.1./ 5.2./ 5.2.1./ 5.2.2./ 5.3.2./ 5.4./ 5.8./ 6.1./ 6.9.1.5./ 6.10.2./6.13.3. | 90% of required reports/documents provided accurate, and on time (specified in each paragraph) each month, with no more than two (2) sets of corrections/edits. All corrections shall be accomplished within two (2) business days. If the delivery time frame is not specifically cited in the individual paragraphs then the two (2) business day time frame applies. 5% of required reports/documents/ correction may exceed due date by not more than 3 business days. |

| | | | |
|---|---|---|---|
| 6 | Maintains a Stable Workforce | 6.9.1.2./ 6.9.2./ | The KTR effectively retains personnel with the appropriate levels of education, experience and expertise to accomplish the tasks. The turnover rate is 15% or less per year (number of personnel replaced or moved without Government direction / total number or personnel assigned). Provides personnel with the required certification upon hire. |
| 7 | Provide Trained and Experienced Personnel | 2.2.5.3./ 2.3.3./ 6.1./ 5.8.1./ 6.9.1.3./ 6.10.1. | KTR personnel must maintain minimum education and certification requirements outlined in the contract, 100% of the time. |
| 8 | Meets Security Requirements | 5.0 – 5.20. | Meets all security requirements, 100% of the time. |
| 9 | Provide Quality Service | IAW the whole PWS. | KTR receives no more than one validated customer complaint/CAR annually per TO. KTR successfully resolves validated customer complaints within 14 business days of receipt, 100% of the time. |
| 10 | Provide Timely Response on Contract Requirements and Requests | 6.1./ 6.10.1. | KTR personnel with decision making authority respond to the CO or COR within 24 hours of the validated emergency, 100% of the time. |

## 4.0. GENERAL REQUIREMENTS.

**4.1. Place of Performance**. Will be on Government installations primarily located in Germany. Principal place of performance is Ramstein AB, Germany; however, the KTR shall provide IT/Communications planning support onsite at the Government installation supported, e.g., Ramstein AB, DE; RAF Lakenheath, UK; RAF Croughton, UK; RAF Mildenhall, UK; RAF Alconbury, UK; RAF Molesworth, UK; Spangdahlem AB, DE; Aviano AB, IT; Lajes Air Field, PT; Incirlik AB, TR (Turkey exception: could be remote support from Ramstein AB, depending on mission requirements). In performance of this PWS the Government may require KTR personnel to travel to units within the European Theater of Operations to include sites located in countries other than the Federal Republic of Germany. If performance is required at a location other than the principal place of performance, i.e., other worldwide Government locations on a temporary basis, travel shall be IAW the Joint Travel Regulation (JTR), and guidelines contained in this PWS. Any time that the circumstances might require to remotely support services, prior written approval from the COR or TR must be obtained.

**4.2. Normal Hours of Performance**. The standard work hours for this contract are 0730 to 1630, Monday through Friday, for a standard 40-hour work week. Host Nation holidays are considered regular work days. KTR who work beyond the standard 40 hour workweek, without other contract provisions, shall do so at no additional charge to the Government. Extended Work Week (EWW) hours, IAW para 4.3.9.must be pre-approved, in writing, by the COR or TR.

**4.2.1. U.S. Federal Holidays.** The following U.S. Federal Holidays are recognized and the KTR is not required to work on these dates, unless otherwise specified in the PWS.

**Table 3. Recognized U.S. Federal Holidays.**

| | |
|---|---|
| New Year’s Day | - January 1 |
| Martin Luther King Day | - 3rd Monday in January |
| President’s Day | - 3rd Monday in February |
| Memorial Day | - Last Monday in May |
| Juneteenth | - June, 19th |
| Independence Day | - July 4th |
| Labor Day | - 1st Monday in September |
| Columbus Day | - 2nd Monday in October |
| Veteran’s Day | - November 11th |
| Thanksgiving Day | - 4th Thursday in November |
| Christmas Day | - December 25th |

4.2.1.1. Holidays, the Government also observes the following days.

4.2.1.1.1. Any other day designated by Federal Statute.

4.2.1.1.2. Any other day designated by Executive Order.

4.2.1.1.3. Any other day designated by the President’s Proclamation.

**4.2.2. On-Call support**, on a case-by-case basis, beyond regular duty hours will be reimbursed IAW paragraph 4.3.8. guidelines.

4.2.2.1. The Government will provide official cellular phones to facilitate after-hours support calls, for which the Government bares the monthly payments. However the usage of these cellular phones is only authorized for official government business and the Government will not pay for any other usage. If misconduct is detected, para 4.4.2. will be applicable and the Government will seek compensation.

**4.3. KTR Reimbursement for Employee Travel Expenses for Temporary Duty (TDY).** Contractor employees may have occasions under this contract to travel from their regular duty location to a temporary duty location, both within and outside the Continental United States.

4.3.1. Travel may be required for the following reasons or other mission requirements:

4.3.1.1. To perform upgrades or base level releases beyond the skillset of local staff or other support personnel.

4.3.1.2. To deploy and implement solutions or system upgrades.

4.3.1.3. To support the USAFE/AFAFRICA enterprise (e.g., on-site support, attending Technical Exchange Meetings, attending/facilitating training sessions, etc.).

4.3.1.4. Support exercises.

4.3.2. Passports and Visa's may be required and it is the KTR responsibility to ensure that these documents are current and valid. All KTR travel shall be coordinated and pre-approved by submitting a Travel Authorization Request (TAR), (RR#: A069) prior to conducting any travel. The TAR will be initiated by the KTR and processed IAW para 4.3.4. below. No travel in support of this contract, regardless of distance, shall be conducted without a TAR and the COR and CO signed Letter of Identification (LOI).

4.3.3. The KTR shall be responsible for obtaining all passenger transportation, lodging and subsistence, both domestic and overseas, required in performance of the TO. Allowable travel costs are described in FAR 31.205-45. If the travel arrangements cause additional costs, which exceed those previously negotiated, written approval by the CO is required prior to undertaking such travel. The JTR does not apply to KTR, however, may be used to aid the CO in making individual decisions regarding travel rules. Cost associated with KTR travel shall be IAW FAR 31.205-46, *Travel Costs*. The KTR shall travel using the lowest cost mode transportation commensurate with the mission requirements. Travel will be reimbursed on a cost reimbursable basis, no profit or fee will be paid.

**Table 4 Travel Notification Timeframes**

| **Duration of TDY in Days** | **Minimum Lead Time Notification** |
|---|---|
| 1 – 2 business days | 3 business days |
| 3 – 7 business days | 5 business days |
| More than 7 business days | 10 business days |

4.3.4. The traveler shall initiate and signed the TAR, obtain the KTR on-site PM and the Section TR coordination and signature. The TR will then submit the TAR to the COR. The TAR shall be in writing and contain at a minimum the name of the traveler, date timeline, location, clearance level and issuing authority, and estimated cost, including per diem IAW the JTR. The COR will create the Letter of Identification (LOI), verify available funding and obtain the COs approval/signature on the LOI. The TDY approval process shall allow a minimum lead time IAW Table 4. Again - no travel shall be conducted without the pre-approved CO signed Letter of Identification (LOI).

4.3.5. The KTR shall be reimbursed IAW FAR 31.205-46. The reimbursement shall be at actual costs incurred, but shall not exceed the maximum allowable rate as set in the JTR and the approved amounts of the LOI. Reimbursement shall be limited to those expenses specifically authorized by the above referenced regulations and pre-approved LOI.

4.3.5.1. The KTR shall be paid a per diem allowance for each day an employee is required to remain over night away from his/her normal duty station, while on official temporary duty status.

4.3.5.2. Transportation and lodging expenses incurred in the performance of temporary duty will be reimbursed at actual costs incurred but shall not exceed the maximum allowable rates as set by the JTR.

4.3.5.3. Meals and Incidental Expenses (M&IE) will be reimbursed at the published M&IE rate for the dates and locations of travel.

4.3.5.4. . When commercial air travel or car rental is authorized, the KTR shall utilize coach, tourist, or similar accommodations.

4.3.5.5. When Government quarters are available and approved, the KTR shall use them.

4.3.5.6. In cases where the TDY purpose requires the Government and the KTR to travel to the same location and the Government provides transportation on a Government Owned Vehicle (GOV), the KTR cannot opt to drive on their own and charge the Government for miles.

4.3.6. Payment for temporary duty expenses will be made on a cost-reimbursable basis. Payment shall be made directly to the KTR upon submission of proper invoices and supporting documentation to the COR. Invoices for reimbursable travel shall be submitted as soon as possible, but within 15 business day from the end of the travel period (RR#: A070).

4.3.7. The KTR shall be reimbursed for travel and per diem expenses IAW the regulations cited above, not to exceed amounts allowable under the JTR. Payment shall be made directly to the KTR on a cost-reimbursable basis, upon submission of proper invoices and supporting documentation to the COR. Invoices for reimbursable travel shall be submitted as soon as possible, but within 15 business days from the end of the travel period (RR#: A070).

4.3.8. On-Call Reimbursement. The KTR shall be reimbursed for any On-Call support beyond regular duty hours. The monthly reporting requirement of the On-Call support provided is met by including this data in the MSR (ref para 2.4.1.3) prior to submission of the reimbursable invoice under the appropriate Contract Line Item Number (CLIN).

4.3.9. Extended Work Week (EWW). Modified work schedules caused by the existence of emergency situations, contingency operations, special events, exercise participation or any other similar circumstances may require KTR employees to operate on a modified work scheduled (>8 hours per day and/or >40 hours per week), including weekends and legal holidays. Any EWW hours must receive Government approval prior to utilizing this option. The request must be in writing and approved by the Lead TR in the Section. The monthly reporting requirement for EWW support provided is met by including this data in the MSR (ref. para 2.4.1.3) prior to submission of the reimbursable invoice under the appropriate contract CLIN.

**4.4. Logistical Support.** The Government will provide logistics support to authorized KTR employees and their dependents to the extent that these services are available at the location where the contract is to be performed and as authorized by current applicable Air Force and European theater regulations, by current applicable international agreements and arrangements, by current policies, and the local installation commander. Lack of availability of any of these services shall not serve as a basis for claims by a KTR against the Government for increased cost of contract performance. Department of Defense Dependents Schools (DoDDS) is available on a space-guaranteed, (KTR) tuition-paying basis only.

4.4.1. **Logistic Support Authorized.** An authorized KTR employee is defined as an employee who has been hired as a consequence of this contract and is employed at least 20 hours per week, in a paid status, on this contract (reference AE Regulation 600-700, I*dentification Cards and Individual Logistics Support*).

4.4.2. **Abuse of Privileges.** The KTR shall include a provision in his employment agreement with these employees to provide for disciplinary actions, or discharge for cause, of the employee for any abuse of privileges authorized to herein. The U.S. Government retains the right to withdraw privileges as a result of KTR employee abuse at no additional cost to the U.S. Government. This provision in no way will prohibit disciplinary action or legal prosecution by either the U.S. Government or the host country government. Services or privileges may be denied on an individual basis at the discretion of the Installation Commander.

4.4.3. The KTR shall assure that upon termination or transfer of any employee who is granted logistic support, action is taken simultaneously with the termination of employment to assure that said employee ceases to have access to the services granted under logistic support. Local policy directs the KTR to turn in Common Access Cards (CAC) or other documents pertinent to or peculiar to the contract or privileges there under to the COR or TR within 1 business days of Termination (SS#: 6, RR#: A071).

**4.5. Government Property Incidental to the Workplace/Services**. The KTR shall ensure accurate control and accountability of all government property IAW Government regulations. The KTR shall perform general and administrative work, in support of this contract, at the Government facility. Information Technology Equipment (ITE) will be provided to each individual KTR who requires for performance under this TO. This is not considered Government Furnished Property as the KTR does not take responsibility for it. No Government Furnished Property will be provided. The services and space provided to the KTR are for official use only. Each individual KTR employee shall be required to sign hand receipts for all ITE that they exclusively use, e.g. all equipment on their desk top. This includes laptops for travel/out of office use. The KTR shall not be required to sign for multiple-user ITE, such as network equipment, network printers, scanners and servers.

4.5.1. Workspace**:** The Government will provide the KTR adequate office workspace to perform the requirements of the TO and all office supplies necessary to perform the requirements of this TO, at all performance locations.

4.5.1.1. Materials and Information. The Government will provide access to relevant government organizations, information, documentation, manuals and associated materials as required and available relative to the assigned responsibilities. The Government will grant access to classified networks as the Government determines necessary and IAW the KTRs clearance level.

**4.6. Non-Personal Services.** This is a TO for non-personal services, defined by FAR Part 37 as "Contract under which the personnel rendering the services are not subject either by the contract's terms or by the manner of its administration to the supervision and control usually prevailing in relationships between the Government and its employees".

4.6.1. The Government will not supervise or otherwise direct KTR employees nor control the method by which the KTR performs the required tasks. The KTR shall not supervise or otherwise direct Government employees, nor shall the KTR supervise employees of other KTR outside the KTR's own subcontracting/ teaming arrangements.

4.6.2. Under no circumstances will the Government assign tasks to, or prepare work schedules for individual KTR employees. It shall be the responsibility of the KTR to manage its employees and to guard against any actions that are of the nature of personal services, or give the perception of personal services, the Governments focus is on the completion of the assigned task. If the KTR feels that any action constitute, or are perceived to constitute personal services, it shall be the KTR's responsibility to notify the TO CO immediately. These services shall not be used to perform work of policy/decision making or management nature, i.e. inherently Governmental functions. All decisions relative to programs supported by the KTR shall be the sole responsibility of the Government.

**4.7. Contractors Identification.** All KTRs and sub-KTR's shall wear a conspicuous article above the waist (e.g., company lanyard, badge, shirt with company logo) so as to distinguish themselves from Government employees. When conversing with Government personnel during business meetings, over the telephone, in all recorded messages including those which are heard by callers attempting to contact KTR employees via answering machines or voice mail, or via electronic mail. KTR/sub-KTR personnel shall identify themselves as such to avoid situations arising where sensitive topics might be better discussed solely between Government employees. KTRs/sub- KTRs shall identify themselves on any attendance sheet or any coordination documents they may review. Identify themselves as KTR personnel at the onset of every meeting, conference or any other gathering attended in support of any service provisions to the Government. Identify themselves as KTR personnel on any correspondence, documents or reports accomplished or sent in support of any service provision to the Government, including but not limited to, correspondence sent via the U.S. Mail, facsimile or electronic mail (e-mail) inclusive of “out-of-office” replies. The KTR shall observe and otherwise be subject to such security regulations as are in effect for the particular premises involved. Electronic mail signature blocks shall identify their company affiliation. KTR occupied facilities on Government installations, such as offices, separate rooms, or cubicles must be clearly identified with the KTR supplied signs, name plates or other identification, showing that these are work areas for KTR and sub- KTR personnel.

4.7.1. The KTR shall designate in writing, an on-the-premises representative to serve as point of contact for the KTR and present to the CO and the COR upon start of the mobilization phase (RR#: A072).

4.7.2. All KTR and sub-KTR employees shall dress to a commercial standard for a professional business work environment.

**5.0. Security Requirements.** Individuals performing work under this TO shall comply with applicable program security requirements as states in this TO PWS.

**5.1. Clearance and Background Checks.** Per paragraph 2.4.3., all KTR employees working directly on any requirements under this contract shall hold at minimum a U.S. Secret clearance prior to performing any services under the TO, except for the DCO support (para 2.2.5.8.), which requires a Top Secret (TS) clearance due to the systems that the KTR will access in order to provide the required support services. The KTR shall comply with the security requirements IAW DD Form 254, *DoD Contract Security Classification Specification*. All KTRs located on military installations shall also comply with Operation Security (OPSEC) requirements as set forth in DoD Directive 5205.02E, DoD *Operations Security (OPSEC) Program*, AFI 10-701, *Operations Security (OPSEC)*, DoDD 5230.25, *Withholding of Unclassified Technical Data From Public Disclosure*, and the International Traffic in Arms Regulation (ITAR). IAW DoDM 5200.2, *Procedures for the DoD Personnel Security Program (PSP)*, DoD military, civilian, consultants, and KTR personnel using unclassified automated information systems, including e-mail, shall have, at a minimum, a completed favorable National Agency Check plus Written Inquiries (NACI). If NATO Secret clearance is required, the applicable employee will be indoctrinated into NATO Secret, as the need arises.

5.1.1. The DCO requirements of this PWS (para 2.2.5.8.) require a TS clearance due to the systems (e.g. World Wide Intelligence Communications System (JWICS)) the KTR will access during the stated support requirements. Access to Sensitive Compartmented Information (SCI), SIPRNET and JWICS are properly marked on the DD 254 accompanying this contract effort.

5.1.2. IAW AFMAN 14-403, *Sensitive Compartmented Information System & Intelligence, surveillance and Reconnaissance Systems Cybersecurity and Governance (SCI)*, para 8.4.2.: “*Access to SCI will be fully justified in the PWS to include the specific types of information needed, whether access to Joint Worldwide Intelligence Communications System (JWICS) is needed, why sanitized intelligence cannot be utilized,and the impact of access is not approved (T-1). Granting SCI access for the purpose of allowing a KTR to transit and SCI area in route to work site or for convenience of assigned personnel is not sufficient justification for approving access*.”

5.1.3. The vast majority of cyber intelligence exists at the TS/SCI level. One of the key roles the KTR fulfills is submitting Requests for Information (RFI) on behalf of subordinate units, USAFE/AFAFRICA-A6 leadership, and external teams operating in theater when they are unable to do so themselves.

5.1.4. The KTRs will receive intelligence updates – again, at the TS/SCI level, from external agencies (e.g. 616 OC, 38 IS, EUCOM JAC, etc.) in order to inform USAFE-AFAFRICA leadership and DCO forces of prominent cyber threats and theater situational awareness.

5.1.5. The KTRs are also required to attend multiple weekly CCMD level TS/SCI Video Teleconferences (VTC). During time of crisis or exercise, these meetings can and will be held daily. Since the KTRs are an integral part of the Cyber section manning, they will require access to these meetings to ensure completed coverage is possible.

**5.2. Employee Clearances.** In addition to the requirements of para 5.1.1., the KTR shall not be authorized access to classified information; access to classified materials, or permitted to perform work on classified projects without proper security clearances, need to know and a signed Standard Form (SF) 312, *Classified Information Nondisclosure Agreement*. All KTR personnel, to include sub-KTR employees, shall sign the SF 312 and provide the original signed letter to the COR within 3 business days of being employed for work on this contract (RR#: A075). The KTR shall be responsible for obtaining employee security clearances to the access required for proper accomplishment of contract requirements. KTR employees whose clearance has been suspended or revoked shall immediately be denied access to classified information and controlled unclassified information (CUI). The KTRs inability to obtain proper employee security clearances shall not constitute an excusable delay in contract performance.

5.2.1. **USAFE Non-Disclosure Agreement (NDA).** In addition to the SF 312, referenced above, which covers the Non-Disclosure of Classified Information, the USAFE NDA must also be completed, it covers access to proprietary information. All KTR personnel, to include sub- KTR employees, shall sign the USAFE NDA agreement and provide the original signed letter to the COR within 3 business days of being employed for work on this contract (RR#: A076). Sample in Appendix D.

5.2.2. **Listing of Employees.** The KTR shall maintain a current listing of all KTR employees to include key personnel. The list shall be grouped by Position Identification (Job Title) and include: the employee's name, Company, Position Title, Clearance Level, Active Certifications and the associated expiration dates (cannot be outdated) and if expired include schedule to update. An updated listing shall be posted within 3 business days of a change in an employee's status or information (RR#: A077).

**5.3. Operations Security**. OPSEC shall be an integral part of this TO to ensure that USAFE-AFAFRICA and subordinate units' critical information is safeguarded. The following tasks will be required of all KTR/ sub-KTR performing any work under this PWS.

5.3.1. The KTR shall provide an OPSEC Plan that outlines the mitigation to be used for this TO, to ensure that procedures are in place to protect critical information.

5.3.2. The KTR shall post the OPSEC Plan NLT 30 days from start of performance (RR#: A001).

5.3.3. The KTR shall work with the USAFE OPSEC office to ensure the OPSEC Plan meets the needs of the government prior to the delivery date.

5.3.4. Personnel will be familiar with and utilize the USAFE-AFAFRICA Critical Information List (CIL) as well as any local CILs, when performing the tasks of this PWS.

5.3.5. Personnel will accomplish the OPSEC 1301 – *OPSEC Fundamentals* located on Government training platform Air Force myLearning: https://lms-jets.cce.af.mil. This will be used to establish a baseline knowledge of OPSEC, its importance, and basic OPSEC techniques.

5.3.6. Those provided with NIPR accounts will encrypt all emails containing work related information. This includes, but is not limited to, work hours and schedules, report of improper payments identified, progress reports, personal information, payment disputes.

5.3.7. Those with SIPR access, communication involving work should be done on the SIPR (e.g., SIPR email) to the max extent possible.

5.3.8. Emails involving work details (word orders, hours, equipment status, limitations, etc.) should be passed as attachments on the DoD SAFE (Secure Access File Exchange website: https://safe.apps.mil if encrypted NIPR email is not available.

5.3.9. Due to the sensitive nature of the information that the KTRs would be working with, a 100% shred policy be implemented regardless of the classification of the material produced except for commercially produced products such as newspapers, magazines, etc.

5.3.10. In addition to the above baseline requirements, personnel will also follow the local OPSEC guidance if TDY to any other locations.

5.3.11. If there are any questions, concerns, please contact your local OPSEC Coordinator or HQ USAFE-AFAFRICA OPSEC Program Manager for additional guidance/assistance.

**5.4. System and Network Authorization Access Requests.** For KTR personnel who required access to DoD, DISA, or AF computing equipment or networks, the KTR shall have the employee, prime or subcontracted, sign and submit a DD Form 2875, *System Authorization Access Request (SAAR)*, to the COR within 2 business days of being employed for work on this contract (RR#: A073).

**5.5. Transmission of Classified Material.** The KTR shall transmit and deliver classified materials/reports IAW DoD 5220.22-M, *National Industrial Security Program Operating Manual*. These requirements shall be accomplished as specified in the PWS.

**5.6. Protection of System Data**. Unless otherwise stated in the TO, the KTR shall protect system design related documents and operational data whether in written form or in electronic form via a network IAW all applicable policies and procedures for such data, including DoD Regulations 5400.7-R, *DoD Freedom of Information Act* and DoDM 5200.2 to include latest changes, and applicable service/agency combatant command policies and procedures. The KTR shall protect system design related documents and operational data at least to the level provided by Secure Sockets Layer (SSL)/ Transport Security Layer (TSL); protected web site connections with certificate and/or user-ID/ password based access controls. In either case, the certificates used by the KTR for these protections shall be DoD approved PKI certificates issued by a DoD approved External Certification Authority (ECA) and shall make use of at least 128-bit encryption.

**5.7. Physical Security**. The KTR shall be responsible for safeguarding all government equipment, information and property provided for KTR use. At the close of each work period, government facilities, equipment, and materials shall be secured. When authorized in writing by the unit of assignment unit commander, KTRs may be authorized to Open/Close the facility. Specific facility Opening/Closing training will be provided by the unit of assignment Unit Security Manager. The KTR shall comply with established security procedures. Security support requiring joint AF and KTR coordination includes, but is not limited to, packaging classified information, mailing and receiving classified materials, implementing emergency procedures for protection of classified information, security checks, and internal security controls for protection of classified material and high value pilferable property.

**5.8. Information Assurance (IA) Technical Considerations.** The KTR shall provide security and information assurance support, protecting information and information systems, and ensuring confidentiality, integrity, authentication, availability, and non-repudiation. The KTR shall ensure that all required reports/documents meet the requirements of DoD Instruction (DoDI) 8500-01, *Cybersecurity*, or the most current standards and guidance that are applicable. This includes A&A activities. The KTR shall provide application services support that are in compliance with and support DoD, USAF and PKI policies. The KTR shall support activities to make applications PKI-enabled (PKE) in order to achieve standardized, PKI-supported capabilities for biometrics, digital signatures, encryption, identification and authentication. The KTR shall assist in defining user and registration requirements of Local Registration Authority (LRA). The KTR shall provide solutions that meet confidentiality, data integrity, authentication, and non-repudiation requirements. KTR solutions shall comply with National Institute for Standards and Technologies (NIST) and Federal Information Processing Standards (FIPS) as applicable. The KTR shall provide applications services support for Security, Interoperability, Supportability, Sustainability, Usability (SISSU) processes, Enterprise Information Data Repository certification. Resulting documentation shall be posted within 2 business days of completion (RR#: A074).

5.8.1. Technical or management certifications are required for anyone performing Information Assurance activities. The KTR shall meet the applicable information assurance certification requirements, including DoD-approved information assurance workforce certifications appropriate for each category and level as listed in the current version of DoD 8570-01-M, *Information Assurance Workforce Improvement Program* (with all current changes) and appropriate operating system certification for information assurance technical positions as required by DoD 8570-01-M, for details see Attachment B, Certification Requirements.

**5.9. Industrial Security**. The KTR shall comply with the provisions of DoD 5220.22M. The KTR shall comply with the security requirements for safeguarding classified information and classified materials, for obtaining and verifying personnel security clearances, for protecting Government property, and for the security of automated and non-automated information systems (AIS) and date are fulfilled. The KTR's AIS shall be protected such that unauthorized disclosure of classified and or sensitive information is prevented.

**5.10. Special Access Programs (SAP).** For the purpose of efficient security administration, Special Access Programs which can include Communications Security (COMSEC), Single Integrated Operational Plan – Extremely Sensitive Information (SIOP-ESI), NATO Information, Restricted Data (RD), Formerly Restricted Data (FRD). The KTR shall process classified materials on Telecommunications Electronics Material Protected from Emanating Spurious Transmissions (TEMPEST) certified computers that have been approved by the Government for transmission of classified materials at the level of the security clearance required.

**5.11. Security Training.** The KTR shall provide employees with training required by DoDM 5200.01, Vol 3, *DoD Information Security Program: Protection of Classified Information* and DODM5200.01_AFMAN16-1404V3, *Information Security Program: Protection of Classified Information*. The KTR shall also provide initial and follow-on training to their KTR personnel who work with Air Force controlled/restricted areas (explained in AFI 31-101, *Integrated Defense (FOUO)*).

**5.12. Restricted Entry Requirements.** The KTR shall arrange for entry into restricted areas, base entry, vehicle passes, and other requirements in conjunction with notification of the Government security activity.

**5.13. COMSEC Notice.** All communications with DoD organizations are subject to COMSEC review. KTR personnel shall be aware that telecommunication networks are continually subject to intercept by unfriendly intelligence organizations. The DoD has authorized the military departments to conduct COMSEC monitoring and recording of telephone calls originating from, or terminating at, DoD organizations. Therefore, KTR personnel are advised that any time they place a call to, or receive a call from, an USAF organization, they are subject to COMSEC procedures. The KTR shall assume the responsibility for ensuring wide and frequent dissemination of the above information to all employees dealing with official DoD information.

**5.14. Pass and Identification Items.** The KTR shall ensure that pass and identification, DoD Contractor Personnel Office (DOCPER) and Trusted Associate Sponsorship System (TASS) items required for contract performance are obtained for employees and non-Government owned vehicles. The KTR is responsible for following pass and identification, DOCPER and TASS processes and Air Force Federal Acquisition Regulation Supplement (AFFARS) clause 5352.242-9001 as amended by theGovernment.

**5.15. Weapons, Firearms and Ammunition.** KTR employees are prohibited from possessing weapons, firearms, or ammunition, on themselves or within their KTR-owned vehicle or privately-owned vehicle while on any installation covered under this contract unless explicitly allowed under USAFE or other applicable installation instructions and/or regulations. For Government installations in Germany, KTR employees shall adhere to USAFE-AFAFRICA Instruction (USAFE-AFAFRICAI) 31-205_IP, *Registrations and Control of Privately Owned Firearms and Other Weapons in Germany*.

**5.16. For Official Use Only (FOUO).** The KTR shall comply with DoD 5400.7-R, Chapter 4 requirements. This regulation sets policy and procedures for the disclosure of records to the public and for marking, handling, transmitting and safeguarding FOUO material.

**5.17. Reporting Requirements.** KTR personnel shall report to an appropriate authority (COR, CO, and Government Office Manager) any information or circumstances of which they are aware that may pose a threat to the security of DoD personnel, KTR personnel, resources, and classified or unclassified defense information.

**5.18. Key Control.** The KTR shall establish and implement methods of making sure all keys issued to the KTR by the Government are not lost or misplaced and are not used by unauthorized persons. All government issued keys will be returned at the end of employment or contract. The KTR shall not duplicate any keys issued by the Government.

5.18.1. The KTR shall immediately report to the COR any occurrences of lost or duplicated keys. In the event keys, are lost or duplicated, the KTR may be required, upon written direction of the CO, to rekey or replace the affected lock or locks without cost to the Government. The Government may, however, at its option, replace the affected lock or locks or perform re-keying and deduct the cost of such from the monthly payment due to the KTR.

5.18.2. The KTR shall not loan issued keys to any other persons nor allow access by use of issued keys to other persons not associated with performance of work at the contract work site.

**5.19. Lock Combinations.** Access lock combinations are protected at the level of the material and or information stored and will be protected from unauthorized disclosure. The Contactor shall control access to all Government provided lock combinations to preclude unauthorized entry. The KTR is not authorized to record lock combinations without written approval by the COR. Records with written combinations to authorized secure storage containers, secure storage rooms, or certified vaults, shall be marked and safeguarded at the highest classification level as the classified material inside the approved containers.

**5.20. Local Area Network (LAN).** The KTR(s) must have at a minimum a valid NACI verified through the Joint Personnel Adjudication System (JPAS) roster of validation from the KTR's security manager, will be provided access to the host base's unclassified computer network and its inherent capabilities including, but not limited to: Internet access, electronic mail, file and print services and network access. The KTR shall be aware of and abide with all Government regulations concerning the authorized use of the Government's computer network including the restriction against using the network to recruit Government personnel or advertise job openings.

## 6.0. Performance Reporting.

**6.1. Quality Control.** The KTR shall develop, implement and maintain a comprehensive quality control plan (QCP) that assures compliance with all requirements of this TO. The QCP shall demonstrate how the KTR plans to ensure quality performance across all products and services under this contract. The quality control plan shall be posted at the start of the actual performance on this TO, future updates shall be posted within 3 business days of updates (RR#: A078). The QCP shall at a minimum document processes for the following:

- Provide quality service
- Quality control review of all required reports/documents
- Providing timely response to contract emergencies
- Providing trained, certified and experienced personnel
- Ensuring timely and effective communications
- Taking preventive and corrective actions
- Meeting reporting requirements

**6.2. Quality Assurance.** The Government will evaluate performance of the services listed in the SS to determine if they meet the performance thresholds. When proper level of performance is not met, the CO will issue a Corrective Action Request (CAR). COR will follow the method of surveillance specified in the QASP. Government personnel will record all surveillance observations. When an observation indicates defective performance, COR will require the KTR to initial the observation. The initialing of the observations does not necessarily constitute concurrence with the observation, only acknowledgement that they have been made aware of the defective performance.

**6.3. Corrective Action Request.** When contract requirements are not met and subsequent corrective action is required, a CAR or electronic equivalent will be initiated by the COR (or the CO) IAW the guidelines listed in the QASP.

**6.4. Performance Deficiency Resolution.** KTR shall take immediate action to correct all Government reported deficiencies and to prevent recurrence of the deficiency.

**6.5. Interference**. The KTR shall support and not interfere with COR, state, federal and otherCO designated personnel in the performance of their official duties.

**6.6. Records Access.** The KTR shall permit the CO or authorized representative access to all records, data and facilities used in the performance of the TO. Access shall be provided within 1 business day of the request and shall be for the purposes of verification of allowable cost, verification of personnel qualifications and items otherwise deemed necessary by theCO.

**6.7. Contract Required Reports.** These required reports are produced from information contained in Government systems, so the Government is only asking for their own data in a specified way. The KTR shall provide the required reports as specified in Table 5. For general posting instructions references paragraph 2.4.5. Delivery instructions and submission timelines are addressed and defined in the associated PWS paragraph listed next to the report in Table 5

**Table 5. Required Reports.**

| Item | Required Report | PWS Para. | Due Dates |
|---|---|---|---|
| **MAIN REPORTS** | | | |
| **ENGINEERING, ARCHITECTURAL DOCUMENTS, REVIEWS, ASSESSMENTS, ANALYSIS, SURVEYS, etc.** | | | |
| A002 | IT Systems Baseline | 2.2.5.7.5. | Post within 5 business days of review. |
| A003 | Technology Roadmap | 2.2.8.1.5. | Post roadmaps within 5 business days of creation or update. |
| **OPERATIONAL & SERVICS MANAGEMENT DOCUMENTATION** | | | |
| A005 | Network Health Assessment Report | 2.2.3.8./ 2.2.3.12. | 2.2.3.8. Post within 3 business days of completion.<br>2.2.3.12. Post NLT the 180th calendar day, or next business day of the year's identified period of performance |
| A006 | Licensing Management | 2.2.7.2./ 2.2.7.3. | 2.2.7.2. Post initial within 90 business days of performance start or 5 business days of review or update Post within 2 business days of review or update. |
| A007 | Asset Inventory | 2.2.7.9. | Post initial documentation within 90 business days of performance start and updates within 5 business days of completion. |
| **OTHER GENERAL REPORTS** | | | |
| **ENGINEERING, ARCHITECTURAL DOCUMENTS, REVIEWS, ASSESSMENTS, ANALYSIS, SURVEYS, etc.** | | | |
| A008 | System Configuration | 2.1.2.9. | Post upon notification of requirement by the COR or TR. |

| | | | |
|---|---|---|---|
| A009 | Assessments and Plans | 2.2.1.5. | Post documents within 2 business days of assessment, unless a time extension has been extended to the KTR, in writing, by the COR or TR. |
| A010 | Procedure Documents | 2.2.2.4. | Post documentation to obtain COR or TR approval prior to release. |
| A011 | Planning Documents | 2.2.3.2. | Post feedback within 5 business days of planning activities. |
| A012 | Architectural Documents | 2.2.3.4. | Post required reports/documents within 5 business days of review, unless a time extension has been extended to the KTR, in writing, by the COR or TR. |
| A013 | Cost Benefit Analysis | 2.2.3.5. | Post documentation within 5 business days of creation or review, unless a time extension has been extended to the KTR, in writing, by the COR or TR. |
| A014 | Network Change Impact Report | 2.2.3.9. | Post report within 10 business days of notification. |
| A015 | Implementation Documentation | 2.2.3.10. | Post required reports/documents within 5 business days of notification. |
| A016 | Performance Engineering & Optimization Report | 2.2.3.11. | Post report within 45 business days of notification. |
| A017 | Meeting Minutes | 2.2.3.14./ 2.2.7.1.2./ 2.3.2.6./ 2.3.2.10/ 6.10.2. | Post documents within 5 business days of event. |
| A018 | Process Documentation | 2.2.4.3./ 2.2.4.6./ | Post documents within 5 business days of creation or review, unless a time extension has been extended to the KTR, in writing, by the COR or TR. |
| A019 | Authorization and Accreditation Documentation | 2.2.5.1.1. | Post Documentation within 5 business days or creation or review, unless a time extension has been extended to the KTR, in writing, by the COR or TR. |
| A020 | Technical Standards and Operation Procedures | 2.2.5.5./ 2.2.5.8.2.2./ 2.2.5.8.2.3./ 2.2.5.8.4./ 2.2.5.8.6./ 2.2.5.8.7./ 2.2.5.8.8. | Post within 3 business days upon creation or modification. |
| A021 | Security Engineering Review | 2.2.5.7.6. | Post within 2 business days of review. |

| | | | |
|---|---|---|---|
| A022 | Requirements Definition | 2.2.5.7.7. | Post within 5 business days of completion. |
| A023 | Security Review | 2.2.5.7.8./<br>2.2.5.7.9. | Post within 5 business days of completion. |
| A024 | Implementation Checklists | 2.2.5.7.11. | Post within 5 business days of completion. |
| A025 | System Analysis | 2.2.8.1. | Post documentation within 5 business days of creation or review, unless a time extension has been extended to the KTR, in writing, by the COR or TR. |
| A026 | Reference & Solution Architectures | 2.2.8.1.7. | Post documents within the first 60 days of the first period of performance. |
| A027 | NMS Baseline Configuration | 2.2.3.15 | Post baseline within 2 business days of creation or update. |
| A028 | Propose Infrastructure & System Topology | 2.3.1.2. | Post within 10 business days of creation or review, or notification of requirement by the COR or TR. |
| A029 | Standards & Procedures for New Technologies | 2.3.1.3. | Post within 10 business days of creation or review, or notification of requirement by the COR or TR. |
| A030 | Proposal Review | 2.3.1.4. | Post within 10 business days of review, or notification of requirement by the COR or TR. |
| A031 | Design Proposal | 2.3.1.5. | Post within 15 business days of creation or notification of requirement by the COR or TR. |
| A032 | Planning and Programming Estimates | 2.3.2.3. | Post within 3 business days of creation, or notification of requirement by the COR or TR. |
| A033 | Manage ETL Processes | 2.3.2.8 | Post within 2 business days of completion. |
| A034 | TMT or eSSS Documents | 2.4.4.1. | Post within 2 business days of creation. |
| A035 | Data Call Products | 2.4.4.2. | Post within 2 business days of any update. |
| **PLANS** | | | |
| A004 | Roadmap or Architecture and CONOPS | 2.3.1. | Post plans within 5 business days within creation or update, unless a time extension has been extended to the KTR, in writing, by the COR or TR. |
| A001 | OPSEC Plan | 5.3.2. | Post plan within 30 days of performance start and distributed in accordance with DD Form 1423-1 |
| A036 | COOP | 2.1.2.13. | Posted within 2 business days of creation or update. |

| | | | |
|---|---|---|---|
| A037 | Assessments and Plans | 2.2.1.5. | Post documents within 2 business days of assessment, unless a time extension has been extended to the KTR, in writing, by the COR or TR. |
| A038 | Implementation Documentation and Plans | 2.2.3.10. | Post required reports/documents within 5 business days of notification. |
| A039 | Project Plan | 2.2.4.7. | Post Plans within 5 business days of notification of the requirement by the COR or TR, unless a time  extension has been extended to the KTR, in writing, by the COR or TR. |
| A040 | Network Architecture Plan | 2.2.5.7.10. | Post within 5 business days of completion. |
| A041 | Configuration Management Plan | 2.2.7. | Post within 2 business days of completion. |
| A042 | Engineering/ Implementation Plan | 2.2.8.1.3. | Post plans within 3 business days of notification of the requirement by the COR or TR, unless a time extension has been extended to the KTR, in writing, by the COR or TR |
| A043 | Impact Analysis & Corrective Action | 2.2.8.1.4. | Post results within 2 business days of completion. |
| A044 | Contingency Plans | 2.2.8.1.6. | Post plans within 5 business days of creation or review, unless a time extension has been extended to the KTR, in writing, by the COR or TR. |
| A045 | Implementation Plan | 2.3.2.1. | Post within 10 business days of creation, review, or notification of requirement by the COR or TR. |
| A046 | Phase In & Final Plan | 2.4.1.4. | Post Phase In within 2 business days of contract award; Final within 5 business days of performance start. |
| A047 | Concept of Operations Plan (CONOPS) | 2.2.5.8.2. | Post within 30 business days of tasking by the COR or TR |
| **PROBLEM / INCICDENT RESOLUTION** | | | |
| A048 | Unresolved Discrepancies | 2.3.1.1. | Post NLT 2 business days after discovery. |
| **OPERATIONAL & SERVICS MANAGEMENT DOCUMENTATION** | | | |
| A049 | Storage Assessment | 2.1.4. | Post results within 2 business days of review. |
| A050 | Storage Justification | 2.1.4.3. | Post within 2 business days of completion. |

| | | | |
|---|---|---|---|
| A051 | IAVM Compliance Assessment | 2.2.5.7.2. | Post within 5 business days of review. |
| A052 | Ports & Protocol Management | 2.2.5.7.4. | Post within 5 business days of review. |
| A053 | Configuration Data | 2.2.7.1.3. | Post within 2 business days of creation/update. |
| A054 | Usage Optimization | 2.2.7.4. | Post within 2 business days of review completion. |
| A055 | Configuration & Network Diagrams | 2.2.7.5. | Post documentation within 2 business days of completion. |
| A056 | Configuration Changes | 2.2.7.6. | Post documentation within 2 business days of completion. |
| A057 | Revision Level of Network Components | 2.2.7.7. | Post documentation within 2 business days of completion. |
| A058 | Name & Addressing Management | 2.2.7.8. | Post documentation within 2 business days of completion. |
| A059 | Site Survey Results | 2.3.2.7. | Post within 5 business days upon survey completion. |
| A060 | System Metrics | 2.3.2.9. | Post within 2 business days of completion, or upon notification of requirement by the COR or TR. |
| A061 | Operational & Service Management Reports | 2.4.1.2. | Post within 5 business days of creation, review, or update, unless a time extension has been extended to the KTR, in writing, by the COR or TR. |
| **CONTRACT / SERVICES MANAGEMENT DOCUMENTATION** | | | |
| A062 | Training Documentation and Guides | 2.2.3.13. | Post documentation within 5 business days of notification. |
| A063 | Certificates | 6.9.3.1. | Post within 5 business days of completion. |
| A064 | On-Call Roster | 2.1.1.1. | Posted on the 1st business day of each month. |
| A065 | ASI | 2.1.1.3. | Submitted 20 business days prior to any upgrade or modification. |
| A066 | Trip Report | 2.4.1.1. | Post within 5 business days upon return. |
| A067 | Monthly Summary Report (MSR) | 2.4.1.3. | Post within 5 business days of the beginning of following month. |
| A068 | CMRA Upload Notification | 6.13.3. | Notify CO and COR via email when reporting is completed. |
| A069 | Travel Authorization Request (TAR) | 4.3.2. | Present to COR or TR IAW Table 4. |

| | | | |
|---|---|---|---|
| A070 | Reimbursable Invoice Supporting Documentation | 4.3.6./4.3.7. | Present to COR or TR within 15 business days upon return. |
| A071 | Employee Termination Letter | 4.4.3./ 6.9.1.5. | Present to COR or TR within 2 business days of Termination. |
| A072 | On-Site POC designation | 4.7.1. | Present to COR or TR upon start of mobilization phase. |
| A073 | System Authorization Access Request (DD 2875) | 5.4. | Present to COR within 2 business days of employment. |
| A074 | IA Technical Considerations | 5.8. | Post within 2 business days of completion. |
| A075 | Classified Nondisclosure Agreement (SF 312) | 5.2. | Present to COR within 3 business days of employment. |
| A076 | USAFE NDA (Appendix D) | 5.2.1. | Present to COR within 3 business days of employment. |
| A077 | Employee Listing | 5.2.2. | Posted within 3 business days of any change in status. |
| A078 | Contractor Quality Control Plan (QCP) | 6.1. | Post within 3 business days of updates. |

**6.8. Contractor Performance Assessment Reporting (CPARS).** The KTR's performance will be monitored and documented monthly on the checklist by the Government and reported annually in CPARS. Performance standards shall include the KTR 's ability to comply with the criteria listed in the Services Summary categories and the overall TO performance.

**6.9. Program Management.**

**6.9.1. Management Requirements.** The KTR manages all aspects of work associated with providing services to the Government via this contract. The KTR shall perform general and administrative work off the Government facility. At a minimum, but not limited to, the KTR shall:

6.9.1.1. Manage employees and performance associated with this TO.

6.9.1.1.1. The KTR shall provide direct supervision of its own employees but shall not supervise or accept supervision from any Government personnel.

6.9.1.2. Maintain a stable workforce.

6.9.1.3. Ensure that the new personnel meet or exceed the stated qualification requirements as stated in this PWS.

6.9.1.4. Common Access Card (CAC). The KTR shall provide changes to the KTR personnel authorized a CAC listing IAW AFFARS clause 5352.242-9001, *CAC for Contractor Personnel* to the COR within 1 business days of any changes (para 4.4.3.). This requirement is met by posting an update to the Employee Listing in para 5.2.2.

6.9.1.5. Provide a Termination Letter on Company Letter Head to the COR within 1 business days of an employee leaving this TO and it must contain the last official working day of the employee under this contract. This Memorandum is a DOCPER requirement (SS#: 6, RR#: A071).

6.9.1.6. Develop and maintain a customer-oriented philosophy, create an environment that improves employee performance, solves programmatic issues and delivers high-quality performance.

6.9.1.7. Respond to CO and/or COR requests within 8 business hours unless otherwise specified by the Government.

6.9.1.8. Identify, document and notify the Government of actual or potential KTR program management problems and deficiencies and report unsolved problems to the CO and COR, as soon as they are detected.

6.9.1.9. Perform corrective actions for all identified KTR program managementproblems and deficiencies IAW time frames specified by the CO.

6.9.1.10. Support periodic meeting and conferences convened at the direction of the CO or COR. The Government will reimburse the KTR for any approved travel requirements to support conferences, meetings, reviews outside the primary duty location commuting areas IAW PWS Para 4.3. – 4.3.7.

6.9.1.11. For situational awareness and planning purposes, the KTR shall notify the COR in writing of planned vacations and other planned absences 30 days in advance, E-mail will suffice.

**6.9.2. Performance Continuity**. The KTR shall notify the COR of personnel changes immediately, but no later than 10 business days prior of any known change (SS#: 6). The KTR shall provide replacement fill status weekly, to the COR until the position(s) is/are filled. The KTR is responsible for continued performance during any absence of employees.

**6.9.3. Training.** The KTR shall ensure KTR employees attend training directly related to TO performance as provided by the Government, or on a cost reimbursable basis as directed/approved by the Government. The training shall be scheduled to ensure mission disruption is at a minimum, which may require alternate work schedules. The KTR shall provide feedback to the Government regarding value of each training event in order to assist the Government with future training planning. If a KTR employee’s training was paid for by the Government and the KTR employee does not remain on task for 365 days following the training, the KTR shall reimburse the Government 100 percent of the training and travel expenses unless replaced with a KTR employee who has already obtained equivalent training. The reimbursement shall not apply to Government downsizing of the requirement or non-execution of an option year.

6.9.3.1. The Government will provide access to computer-based training websites for any HHQ-required training. The KTR employees shall maintain currency in all required HHQ-required training; i.e. Cyber Awareness, Force Protection, Human Relations, etc. and shall post certificates within 5 business days of completion (RR#: A063).

6.9.3.2. It is the KTRs responsibility to ensure that the required KTR certifications are valid and the KTR shall ensure that renewal training for the required certification is scheduled appropriately, to ensure required expertise services are covered.

### 6.10. Task Order Management.

6.10.1. The KTR shall establish and provide qualified workforce capable of performing the required tasks. The KTR shall designate in writing an onsite point of contact (POC), who shall be the primary representative responsible for all work awarded under this contract, participating in Program Management Reviews and ensuring all standards referenced herein are adhered to and shall hold Project Management Professional (PMP) certification. The KTR shall provide the appointment/update in writing (e-mail acceptable), within 2 business days of contract award or upon any change, to the COR (SS#: 7 &10). The KTR shall support stakeholder meetings, staff meetings and other program meetings as required.

6.10.1.1. During the mobilization phase, this POC will already establish communications with the government customer and obtain adequate familiarization with the work environment and work load, to ensure a smooth transition at the actual start of performance on this TO.

6.10.2. **Conferences and Meetings.** During the performance of this TO, the KTR shall support/attend stakeholder meetings, engineering meetings and other program meetings, as approved by the COR, in a manner that does not conflict with other taskings. The frequency of these meetings is cited throughout the PWS, and the overall intended location of the meetings will be Ramstein AB, Germany. These meetings can be held onsite or via teleconference. The KTR shall post meeting minutes within 5 business days after the meeting (RR#: A017).

6.10.3. The KTR shall use key performance parameters to monitor work performance, measure results, ensure delivery of contracted services and reports, support management and decision-making and facilitate communications. The KTR shall identify risks, resolve problems and verify effectiveness of corrective actions. The KTR shall institute and maintain a process that ensures problems and action items discussed with the Government are tracked through resolution and shall provide timely status reporting. Results of KTR actions taken to improve performance should be tracked, and lessons learned incorporated into applicable processes. The KTR shall establish and maintain a documented set of disciplined, mature, and continuously improving processes for administering all contracts and TO efforts with an emphasis on cost-efficiency, schedule, performance, responsiveness and consistently high-quality services delivery. The KTR shall provide transition plans as required. This requirement is met by posting an updated QCP (ref. paragraph 6.1.).

### 6.11. Mobilization Period.

6.11.1. The primary purpose of the mobilization period is to allow for the host nation and DoD Contractor Personnel Office (DOCPER) review and approval of the contract, TOs (if applicable) and individual employees (up to 8 weeks). Requirements and timelines for Germany are at: https://ecops.ext.eur.army.mil/. All KTR employees working in Germany during the mobilization period are NOT eligible for an Identification Card and logistics support, until Technical Expert Status Accreditation (TESA) is granted by the German Government. As soon as TESA is granted and the employee is on site, will the Government consider the position as officially filled. Once on site each approved KTR employee will be provided a "Base Support Memorandum (BSM) which will provide access to additional tax-free services. KTR personnel working in Germany longer than 90 days without the proper status are deemed "ordinarily residents", and may be liable to taxation by the German Government.

6.11.2. The KTR shall have 90 days to prepare and become fully operational to assume complete contract responsibility for TOs awarded. The KTR shall accomplish such tasks as becoming familiar with work sites, hiring and training personnel, meeting with government staff members and transitioning with outgoing KTR.

**6.12. Performance Requirements unique for the Federal Republic of Germany.** DOCPER implements the Agreements of 27 March 1998, and the Agreements of 29 June 2001, signed by the U.S. Embassy and German Foreign Ministry, establishing bilateral implementation of Articles 72 and 73 of the Supplementary Agreement (SA) to the NATO Status of Forces Agreement. These 2 Articles govern the use in Germany of DoD KTR employees as Technical Experts (TE), Troop Care (TC) providers, and Analytical Support (AS) KTR personnel. This contracts will be accredited under Article 73 and the applications of individuals that seek TE status under this contract shall be submitted to DOCPER. Simultaneously with this TESA status application, DOCPER provides NATO Status of Forces Agreement (SOFA) status. Basic guidance on the TE process is provided in Army in Europe Regulation (AE Reg) 715-9, *Contractor Personnel in Germany – Technical Expert, Troop Care and Analytical Support Personnel*, available at AEPUBS: https://www.aepubs.eur.army.mil//, for further details and assistance see DOCPER's Internet website: ecops.ext.eur.army.mil:

6.12.1. In order to obtain contract approval from DOCPER, the KTR shall submit all sub-KTR agreements, which are part of the Government's Contract Notification package to DOCPER. The KTR shall submit TESA application packages for any employee for which status is sought within 3 business days of the individual being hired.

6.12.2. No individual application packages can be submitted until the overall contract approval from the German Government is received. Then applications shall be submitted by the KTR via DOCPER's automated system: European Contractor Online Processing System (ECOPS), see link above to DOCPER. An authorized KTR employee is defined as an employee who has been hired as a consequence of this contract and is employed 40 hours per week of this contract.

6.12.2.1. AE Regulation 600-700, *Identification Cards and Individual Logistic Support* defines a full time employee as “An employee who works 20 hours or more a week in a paid status.” A civilian employee must therefore work 20 hours or more per week in order to be eligible to receive Individual Logistic Support (ILS). DOCPER will apply the same standard to contracted employees applying for NATO Status of Forces Agreement (SOFA) status. It should be noted, that under the requirements of the Exchange of Notes a contracted employee accorded NATO SOFA status must exclusively serve the U.S. Forces. No additional employment outside the U.S. Forces or self- employment is permitted.

6.12.3. Details, guidance and assistance on other legal ways to bring on temporary support can also be obtained through the DOCPER link above.

6.12.4. **Current CAC procedures for Germany:**

6.12.4.1. Upon TESA, ECOPS will issue the DD Form 1172-2, *Application for DoD Common Access Card* and AE 600-77A, *Request for Issue of Status of Forces Agreements (SOFA) Identification*.

6.12.4.2. The COR works with the Trusted Agent (TA) on the KTR employees record in Trusted Associate Sponsorship System (TASS). This process includes a Security Officer coordination.

6.12.4.3. Once the TASS process is completed, the KTR employee can take the ECOPS issued DD 1172-2 and AE 600-77A to the local Pass & ID office and the CAC cards for the KTR employee and possible dependents will be issued.

6.12.5. The contract price shall not be subject to an economic adjustment with regard to TESA in the event that:

6.12.5.1. The contract, or any positions submitted for TESA identified in the KTR’s proposal or during the life of the contract are disapproved for TESA.

6.12.5.2. Any or all KTR employees are denied TESA.

6.12.5.3. TESA accreditation is rescinded during the life of the contract.

6.12.6. The KTR shall allow German government authorities to visit the KTR’s work areas for the purpose of verifying the status of positions and personnel as TE employees. Such visits will not excuse the KTR from performance under this contract or results in increased costs to the Government.

6.12.7. The KTR shall allow German government authorities to visit the KTR’s work areas for the purpose of verifying the status of positions and personnel as TE employees. Such visits will not excuse the KTR from performance under this contract or results in increased costs to the Government.

**6.13. Contractor Manpower Reporting.** IAW the basic PWS

**6.14. Records, Files, Documents.** All physical records, files, documents, and work papers, provided and/or generated by the Government and/or generated for the Government in performance of this PWS, maintained by the KTR which are to be transferred or released to the Government or successor KTR, shall become and remain Government property and shall be maintains and disposed of IAW AFI 33-322, *Records Management and Information Governance Program and Responsibilities*, the Federal Acquisition Regulation, and/or Defense Federal Acquisition Regulation Supplement, as applicable. Nothing in this section alters the rights of the Government or the KTR with respect to patents, data rights, copyrights, or any other intellectual property or proprietary information as set forth in any other part of this PWS or the IT Professional Support and Engineering Services contract of which this PWS is a part (including all clauses that are or shall be included or incorporated by reference into that contract.)

**6.15. Section 508 of the Rehabilitation Act.**

6.15.1. The KTR shall meet the requirements of the Access Board’s regulations at 36 Code of Federal

Regulation (CFR) Part 1194, particularly 1194.22, which implements Section 508 of the Rehabilitation Act of 1973, as amended. Section 508 (as amended) of the Rehabilitation Act of 1973 (20 United States Code (U.S.C.) 794d) established comprehensive requirements to ensure: (1) Federal employees with disabilities are able to use information technology to do their jobs, and (2) members of the public with disabilities who are seeking information from Federal sources will be able to use information technology to access the information on an equal footing with people who do not have disabilities.

**6.16. Documentation and Data Management.**

6.16.1. The KTR shall establish, maintain, and administer a Documentation Library IAW para 2.4.5. for collection, control, publishing, and delivery of all program documents. This Library shall include but not be limited to the following types of documents: Status Reports, Audit Reports, Agendas, Presentation Materials, Minutes, Contract Letters, and TO Proposals. This Library shall provide the Government with electronic access to this data, including access to printable reports.

6.16.2. The Government will furnish or make available to the KTR any documentation/ material deemed necessary to accomplish the TO requirements.

**6.17. Performance of Services During Crisis Declared by the President of the United States, the Secretary of Defense, or Overseas Combatant Commander.** IAW DODI 1100.22, *Policy and Procedure for Determining Work Force Mix*, paragraph 5b, it has been determined that this requirement is not ME, exceptions cited in para 2.4.2. which only controls access to the regular work site.

**6.18. Organizational Conflict of Interest (OCI).** Whenever the Government solicits information from the KTR for the purposes of issuing a potential TO (or, if the Government issues a TO without first soliciting information from the KTR), unless the TO states that it is exempt from the OCI provisions, the KTR shall promptly review the services ordered prior to commencing performance and inform the TO CO, in writing, of any pre-existing circumstances which might create a conflict of interest under the OCI provisions of this contract with a plan to mitigate conflicts. In such event, the Government may, in its sole discretion, either cancel the TO at no-cost to the Government or grant a waiver to the OCI provisions and direct the KTR to proceed with performance. This process will also apply over the life of the TO.

**6.19. Constraints.**

6.19.1. The Government, during the course of this contract, may encounter the following conditions:

6.19.1.1. **Surge Support:** The Government may require surge support during the base or any option period, and surge modifications will be within the scope of the contract and provide increased support for the defined task areas of this PWS. In pursuit of DoD’s, SAF-CIO’s unpredictable mission updates/changes a situation requiring an increased level of services and/or support over a compressed schedule of time could apply. Normally, surge requirements are of short duration, with an estimated time line from one to six months. Surge requirements shall be accomplished as required under the Task Order. It is envisioned that surge and optional CLINs be utilized to address such unpredictable future organizational requirements via Task Order modifications.

6.19.1.2. **Draw-down:** A situation requiring the reduction of services and/or support within the scope of the TO resulting from, but not limited to, completion/deletion/transfer of programs or Government directed reductions.

**6.20. Environment.**

**6.20.1. Conformance with Environment Management Systems (EMS).**

6.20.1.1. The KTR shall perform work under this contract consistent with the relevant environmental policy and objectives identified in the installation Environment Management System applicable for your contract. The KTR shall perform work in a manner that conserves water, energy and other resources to the maximum extent feasible and ensure minimum production of waste as possible, giving preference to recycling and reutilization opportunities.  Furthermore, the KTR shall give preference to less toxic materials whenever available and still reliable for their work. In the event an environmental nonconformance or noncompliance of host nation and USAF environmental laws and regulations associated with the contracted services is identified, the KTR shall take corrective and/or preventative actions. In the case of a noncompliance, the KTR shall respond and take corrective action immediately. In the case of a nonconformance, the KTR shall respond and take corrective action based on the time schedule established by the Environment Management System Coordinator.  In addition, the KTR shall ensure that their employees are aware of the environmental management system on base and how these requirements affect their work performed under this contract.

6.20.1.2.  All on-site KTR personnel shall receive the installation Environment Management System awareness level information.

**6.20.2.  Conformance with Environmental Requirements.**

6.20.2.1.  The KTR shall perform all work IAW applicable German and US Air Force environmental laws, regulations and operating standards, including but not limited to the Final Governing Standards (FGS) for Germany. The KTR shall be immediately capable of understanding and addressing environmental laws and regulations as they pertain to work performed under this contract.

6.20.2.2.  The FGS for Germany and other important environmental laws & requirements applicable for all KTRs working on base can be found at the Environment Management System SharePoint Website https://ice.usafe.af.mil/sites/EMS/Legal%20%20Other%20Requirements/Forms/AllItems.aspx

6.20.2.3.  The PWS requirements, including technical documentation review revealed that this PWS does not require the KTR to use Class I Ozone Depleting Chemicals (ODC) identified in the Air Force policy in performance of the contract, nor does it require the delivery of the Class I ODC's in any part of any services.

# APPENDIX A- ABBREVIATIONS AND REFERENCES

## Abbreviations and Acronyms

| | |
|---|---|
| A&A | Authorization and Accreditation |
| A6 | Communications Directorate |
| AB | Air Base |
| ACC | Air Combat Command |
| AF | Air Force |
| AFCYBER | Air Force Cyber |
| AFLCMC | Air Force Life Cycle Management Center |
| AIS | Automated Information Systems |
| AS | Analytical Support |
| ASI | Authorized Service Interruptions |
| BSM | Base Support Memo |
| C4 | Command, Control, Communications, and Computer |
| C4I | Command, Control, Communications, Computer and Intelligence |
| CAC | Common Access Cards |
| CAM | Coordinated Alert Messages |
| CAR | Corrective Action Request |
| CARM | Critical Asset Risk Assessment |
| CCB | Change Control Board |
| CCC | Cyberspace Capabilities Center |
| CCIE | Cisco Certified Internetworking Expert |
| CCMD | Combatant Commander |
| CCNP | Cisco Certified Network Professional |
| CCT | CISCO Certified Technician with Collaboration |
| CDR | Call Detail Record |
| CFR | Code of Federal Regulation |
| CIL | Critical Information List |
| CIO | Chief Information Officer |
| CLIN | Contract Line Item Number |
| CMRA | Contractor Manpower Reporting Application |
| COAS | Consolidated Operator Answering System |
| CO | Contracting Officer |
| COMSEC | Communications Security |
| CONOPS | Concept of Operations |
| COOP | Continuity of Operations Plan |
| COR | Contracting Officer Representative |
| COS | Cyber Operations Squadron |
| CPARS | Contractor Performance Assessment Reporting |
| CRM | Customer Relationship Management |
| CSfC | Commercial Solutions for Classified |
| CTO | Command Tasking Order |
| CUCM | Cisco Unified Communications Manager |
| CUI | Controlled Unclassified Information |
| CYBERCOM | Cyber Command |

| | |
|---|---|
| DCO | Defensive Cyberspace Operations |
| DCOI | Data Center Optimization Initiative |
| DISA | Defense Information Systems Agency |
| DOCPER | DoD Contractor Personnel Office |
| DoD | Department of Defense |
| DoDDS | Department of Defense Dependents School |
| DE | Germany |
| DevSecOps | Development, Security and Operation |
| DR | Disaster Recovery |
| DRP | Disaster Recovery Plan |
| E&I | Engineering and Installation |
| ECA | External Certification Authority |
| EIC | European Infrastructure Consolidation |
| eMASS | Enterprise Mission Assurance Support System |
| EMS | Environment Management System |
| ERI | European Reassurance Initiative |
| eSSS | Electronic Staff Summary Sheet |
| ETL | Engineering Technical Letter |
| EVM | Enterprise Virtualization Management |
| EWW | Extended Work Week |
| FAR | Federal Acquisition Regulation |
| FGS | Federal Governing Standards |
| FIPS | Federal Information Processing Standards |
| FMA | Functional Mission Analysis |
| FOC | Full Operational Capability |
| FOUO | For Official Use Only |
| FRAGO | Fragmentary Order |
| FRD | Formerly Restricted Data |
| FY | Fiscal Year |
| GOV | Government Owned Vehicle |
| GSU | Geographically Separated Unit |
| HAF | Headquarter Air Force |
| HHQ | Headquarter Air Foce |
| HQ | Headquarter |
| IA | Information Assurance |
| IAM | Information Assurance Manager |
| IAT | Information |
| IAVM | Information Assurance Vulnerability Management |
| IAW | In accordance with |
| ILS | Individual Logistic Support |
| INFOCON | Information Operations Condition |
| IOC | Interim Operational Capability |
| IP | Internet Protocol |
| IPAM | IP Address Management |
| IPT | Integrated Product Team |
| IT | Information Technology |

| | |
|---|---|
| ITAM | Information Technology Asset Management |
| ITAR | International Traffic in Arms Regulation |
| ITE | Information Technology Equipment |
| ITIL | Information Technology Infrastructure Library |
| ITSM | IT Service Management |
| ITSS | Information Technology Support Services |
| JPAS | Joint Personnel Adjudication System |
| JTR | Joint Travel Regulation |
| JWICS | Joint Worldwide Intelligence Communications System |
| KTR | Contractor |
| LOI | Letter of Identification |
| LRA | Local Registration Authority |
| LSC | Local Session Controller |
| M&IE | Meals and Incidental Expenses |
| MAA | Mission Assurance Assessment |
| MAJCOM | Major Command |
| MCCC | MAJCOM Communications Coordination Center |
| MDT | Mission Defense Team |
| ME | Mission Essential |
| MOB | Main Operating Base |
| MPLS | Multi-protocol Label Switching |
| MPTO | Methods and Procedures for Technical Orders |
| MRT-C/MM | Mission Relevant Terrain-Cyber/ Mission Mapping |
| MS | Microsoft |
| MSR | Monthly Summary Report |
| NACI | National Agency Check plus Written Inquiries |
| NATO | North Atlantic Treaty Organization |
| NDA | Non-Disclosure Agreement |
| NIPR | Non-Classified Internet Protocol Routed |
| NIPRNet | Non-Classified Internet Protocol Routed Network |
| NIST | National Institute for Standards and Technology |
| NLT | Not Later Than |
| NMS | Network Management System |
| NSA | National Security Agency |
| O&M | Operations and Maintenance |
| OCI | Organizational Conflict of Interest |
| ODC | Ozone Depleting Chemicals |
| OPORD | Operational Order |
| OPSEC | Operations Security |
| OPT | Operational Planning Team |
| PaaS | Platform as a Service |
| PCF | Pivotal Cloud Foundry |
| PKE | PKI Enabled |
| PKI | Public Key Infrastructure |
| PM | Project Management |
| PMI | Project Management Institute |
| PMP | Project Management Professional |

| | |
|---|---|
| POA&M | Plan of Action and Milestones |
| POC | Point of Contact |
| PSP | Personnel Security Program |
| PWS | Performance Work Statement |
| QASP | Quality Assurance Surveillance Plan |
| QCP | Quality Control Plan |
| RAF | Royal Air Force |
| RD | Restricted Data |
| RFI | Request for Information |
| RMF | Risk Management Framework |
| SA | Supplementary Agreement |
| SAAR | System Access Request |
| SAF | Secretary of the Air Force |
| SAFE | Secure Access File Exchange |
| SAP | Special Access Programs |
| SBC | Session Border Controller |
| SCI | Sensitive Compartmented Information |
| SDLC | System Developmental Lifecycle |
| SIOP-ESI | Single Integrated Operation Plan - Extremely Sensitive Information |
| SIP | Session Initiation Protocol |
| SIPR | Secret Internet Protocol Routed |
| SIPRNet | Secret Internet Protocol Routed Network |
| SISSU | Security, Interoperability, Supportability, Sustainability, Usability |
| SOFA | Status of Forces Agreement |
| SOO | Statement of Objectives |
| SOW | Statement of Work |
| SPO | System Program Office |
| SQL | Structured Query Language |
| SRST | Survivable Remote Site Telephony |
| SS | Service Summary |
| SSL | Secure Sockets Layer |
| STIG | Security Technical Implementation Guides |
| TA | Trusted Agent |
| TAR | Travel Authorization Request |
| TASKORD | Tasking Order |
| TASS | Trusted Associate Sponsorship System (formerly CVS) |
| TC | Troop Care |
| TCA | Task Critical Asset |
| TDM | Time Division Multiplexing |
| TDY | Temporary Duty |
| TE | Technical Expert |
| TEMPEST | Telecommunications Electronics Material Protected from Emanating Spurious Transmissions |
| TESA | Technical Expert Status Accreditation |
| TMT | Tasking Management Tool |
| TO | Task Order |
| TR | Technical Representative |

| | |
|---|---|
| TS | Top Secret |
| TSL | Transport Security Layer |
| UC | Unified Communications |
| UCCX | Cisco Unified Contact Center Express |
| UCS | Cisco Unified Computing System |
| UK | United Kingdom |
| U.S. | United States |
| U.S.C. | United States Code |
| USCYBERCOM | United States Cyber Command |
| USAF | United States Air Force |
| USAFE-AFAFRICA | United States Air Forces in Europe/Air Forces in Africa |
| USAFRICOM | United States Africa Command |
| USEUCOM | United States European Command |
| VDI | Virtual Desktop Infrastructure |
| VG | Voice Gateway |
| VGR | Voice Gateway Router |
| VoIP | Voice over Internet Protocol |
| VoSIP | Voice over Secure Internet Protocol |
| VPN | Virtual Private Network |
| VSAN | Virtual Storage Area Network |
| VTC | Video Teleconference |
| VXLAN | Virtual Extensible Local Area Network |
| WBS | Work Breakdown Structure |

**REFERENCES**

**Publications:**

DoDI 1100.22, *Policy and Procedure for Determining Work Force Mix*

DoDM 5200.01 Vol 3, *DoD Information Security Program: Protection of Classified Information*

DoDM5200.02, *Procedures for the DoD Personnel Security Program (PSP)*

DoDD 5205.02E, *DoD Operations Security (OPSEC) Program*

DoD 5220.22-M, *National Industrial Security Program Operating Manual*

DoDD 5230.25, *Withholding of Unclassified Technical Data from Public Disclosure*

DoD Reg 5400.7-R, *DoD Freedom of Information (FOIA) Act*

DoDI 8500-01, *Cybersecurity*

DoDM 8570.01M, *Information Assurance Workforce Improvement Program*

AFI 10-701, *Operations Security (OPSEC)*

AFMAN14-403*, Sensitive Compartmented Information System & Intelligence, Surveillance and Reconnaissance Systems Cybersecurity and Governance*

DODM5200.01_AFMAN16-1404V3, *Information Security Program: Protection of Classified Information*

AFI 17-140, *Air Force Architecting*

AFMAN 17-1203, *Information Technology (IT) Asset Management (ITAM)*

AFI 31-101, *Integrated Defense (FOUO)*

AFI 32-1023**,** *Designing and Constructing Military Construction Projects*

AFI 33-322, Records *Management and Information Governance Program*

AFI 63-138, *Acquisition of Services*

USAFEI 10-505, *Geographically Separated Unit and Tenant Support*

USAFE-AFAFRICAI 31-205_IP, *Registration and Control of Privately Owned Firearms and Other Weapons in Germany*

AE Reg 600-700, *Identification Cards and Individual Logistic Support*

AE Reg 715-9, *Contractor Personnel in Germany - Technical Expert, Troop Care and Analytical Support Personnel*

Air Force Engineering Technical Letter 02-12, *Communications and Information System Criteria for Air Force Facilities*

MPTO 00-33A-1001, *General Cyberspace Support Activities and Management Procedures and Practice*

ITAR - *International Traffic in Arms Regulation*

**Forms**

DD Form 254, *DoD Contract Security Classification Specification*

DD 1172-2, *Application for DoD Common Access Card*

DD Form 1423-1, *Contract Data Requirements List*.

DD 2875, *System Authorization Access Request (SAAR)*

SF 312, *Classified Information Nondisclosure Agreement*

AE 600-77A, *Request for Issue of Status of Forces Agreement (SOFA)*

# APPENDIX B: EDUCATION, EXPERIENCE AND CERTIFICATION REQUIREMENTS

**B.1. General Requirements.** In order for a KTR employee to qualify for TESA status under DOCPER (see paragraph 6.12.), they must meet the following required baseline education/experience requirements. These requirements are set by the German government and the U.S. Government does not control them or have the option to approve waivers. In addition, if the KTR applicant does not meet the specified certification position requirements listed below, they will not receive COR coordination on the DOCPER application.

B.1.1. A bachelor's degree plus 3 years of recent specialized experience; OR, an associate's degree plus 7 years of recent specialized experience; OR, a major certification plus 7 years of specialized experience; OR, 11 years of recent specialized experience.

B.1.2. .Ensure all KTR personnel granted elevated systems privileges or performing cybersecurity functions on USAFE-AFAFRICA systems/networks are trained and certified in accordance with DoD Manual 8570.01M, *Information Assurance Workforce Improvement Program,* i.e. CompTia Network +CE, CompTia Security +CE or equivalent.

B.1.3. Ensure all KTR personnel performing program management tasks shall possess a Project Management Professional (PMP) certification, issued by the Project Management Institute (PMI)

**B.2. Certification Requirements.** As proof of adequate proficiency in each technology area, the KTR staff shall possess the following current technical certifications:

B.2.1. Network Engineers:

- Two Tier-III Network Engineers with Cisco Certified Internetworking Expert (CCIE) certification.
- One Data Center Infrastructure Engineer with Cisco Certified Network Professional (CCNP) Data Center or higher certification.
- One CCIE with minimum of 2 years Multi-protocol Label Switching (MPLS) experience. CCIE may be any type (e.g., Routing and Switching, Security, or Service Provider) but must have a minimum of 2 years of experience in engineering, configuring, and troubleshooting MPLS.
- One SecureView Infrastructure Engineer with Cisco Certified Network Professional Security (CCNP Security) certification.

B.2.2. Unified Communications (UC) Engineers:

- Two (2) Cisco Certified Network Professional with Collaboration (CCNP Collaboration) certification or higher. Current and Maintained.
- Three (3) Cisco Certified Technician with Collaboration (CCT Collaboration) certification or higher, with three (3) years or more of recent specialized experience working enterprise-level support implementing and operating Cisco collaboration core technologies such as Cisco Unified Communications Manager (CUCM), Cisco Unified Contact Center Express (UCCX), and Cisco Unity. Current and Maintained.

B.2.3. SharePoint - Enterprise level Certification

B.2.4. Windows Server - administrator certification

B.2.5. VMWare Ver 6.0 or newer Certification

B.2.6. VMWare Virtual Desktop Infrastructure certifications

B.2.7. Minimum of Information Assurance Technology (IAT) Level II for all Employees (required for elevated administration rights)

B.2.8. DoD Information Assurance Manager (IAM) Level III Certifications (Cyber surety requirements.)

B.2.9. Microsoft Customer Relationship Management (CRM) administration certification

B.2.10. In addition to the TESA education and experience requirements, engineer positions require a minimum of 3 years of experience with enterprise-level support.

B.2.11. In addition to theTESA education and experience requirements, Help Desk require a minimum of 1 year experience with enterprise-level support.

B.2.12. Dec Ops Engineer – Experience with cloud providers and infrastructure as a service. Minimum 2 years experience with a platform as a service product such as Cloud Fountry, Heroku, Elasric Beanstalk, or similar. Experience in using Docker, Kubernetes or container orchestration. Experience with Chef, Puppet, BOSH, Terraform or related automation/ orchestration tools. Clear understanding of could service and deployment models. Comfortable in Java (or equivalent languages), with significant experience with Java SE and Java EE and Experience with the Spring Framework.

# APPENDIX C: WORKLOAD ESTIMATES

**C.1. Workload Estimates:** The quantities, as stated herein, are estimates and, as such, are subject to variations are not all conclusive. These estimates are provided for the KTR to understand the full scope of workload to be performed; complete requirement descriptions are outlined further throughout the PWS. The system currently supports 84 locations across Europe and Africa with 40,000 customers using 28,000 connected devices distributed among twelve call clusters. USAFE- AFAFRICA also supports 15,000 VoSIP customers on a separate call cluster. VDI clients and SecureView laptops hosted from virtual environments. The intent of this contract is not to administer end-user applications other than VDI. The table below lists overall functions and the tasks. The column titled “Est Monthly Hrs.” represents the estimated monthly total of hours spent performing the task. The column titled “Number of Events” represents the estimated number of occurrences of that event within a month. The KTR shall be responsible for providing feedback to the Government if these workload estimates are found to have a range variation of greater than 15%. These figures are based on historical data and are not intended to alter the priced nature of performing this work. The Government Workload Estimate is only provided for planning purposes, and the KTR is responsible for the technical solution they propose with their estimate. The contract will be awarded upon their proposal to perform to required PWS tasks, and not to achieve the Government Estimated Hours or events.

## C.2. USAFE/AFRICA WORKLOAD ESTIMATE FOR ITSS-II TASK ORDER

**ANNUAL HOURS**

**Please note that this is a performance based contract. While the Government is providing estimate/historical FTE data, a proposal that is extremely low or high will have to be justified/explained in the proposal submitted.**

| | **Estimate** | **# of Events (Annual)** | **Base Aug XX – July XX** | **Option 1 Aug XX – July XX** | **Option 2 Aug XX – July XX** | **Option 3 Aug XX – July XX** | **Option 4 Aug XX – July XX** | **Comments** |
|---|---|---|---|---|---|---|---|---|
| **TIER 2 MAJCOM UNIQUE SYSTEMS** | | | | | | | | |
| **TIER 2 Unified Communications** | | | | | | | | |
| Incident, Problem, Change Support | 5.5 FTEs ([0.5x CCNP-Collaboration, 3x CCT Collaboration, 2x System Administrator) | 260 | Included below | Included below | Included below | Included below | Included below | |
| UC System Administration Task | | 180 | 1000 | 960 | 960 | 1160 | 1460 | |
| UC System Administration | | 100 | 1000 | 1000 | 2000 | 2000 | 2000 | |
| System Storage Capacity Management | | 12 | 480 | 480 | 40 | 40 | 40 | |
| CUCM | | 300 | 2000 | 2000 | 2000 | 2000 | 2000 | Support managed Call Clusters |
| Automated Call Distribution | | 500 | 500 | 500 | 500 | 500 | 500 | |
| Voice Gateway Routers | | 150 | 480 | 200 | 1500 | 1500 | 1500 | Option 3 –see Tech Refresh or US System redesign |
| Analog Voice Gateway | | 150 | 960 | 200 | 200 | 300 | 300 | Option 3 – see Tech refresh or UC system redesign |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Public Key Administration (all support systems) | | 300 | 100 | 960 | 640 | 500 | 500 | Project at a min. of 1 and max of 2 PKI certificate updates on all servers during contract period |
| Legacy Voice Transition | | 5000 | 960 | 960 | 1960 | 1960 | 1960 | Project # of events to decrease as user end points transition to UC IP Solutions |
| UC Training /Knowledge Transfer | | 4 | 320 | 320 | 100 | 100 | 100 | 4x one week training sessions, incl. 5 days for each session to prepare & coordinate |
| UC Upgrades (CUCM,CUC, UCCX) | | 12 | 200 | 3000 | 660 | 500 | 200 | Project two major software upgrades during contract period |
| Enhanced E911 | | 20 | 40 | 40 | 40 | 40 | 40 | Connectivity support with CUCM |
| CDR and Billing System Support | | 16 | 200 | 200 | 200 | 200 | 200 | |
| COAS Servers | | 0 | 0 | 0 | 100 | 100 | 100 | Support OAS related servers |
| Virtual Desktop Infrastructure O&M | 2 FTE VDI Administrators | 200 | 490 | 2000 | 4000 | 4000 | 4000 | Option 1 will absorb and existing contract position |
| VDI Training | | 4 | 320 | 320 | 320 | 320 | 320 | 4 x one week training sessions- include 5 days for each session to prepare & coordinate |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Tier 2 Collaboration Services** | | | | | | | | |
| TMT O&M / Administration | 3 System Administrators 1 Database Administrator | 0 | 0 | 0 | 2000 | 2000 | 2000 | |
| TMT Upgrade incl. Share Point | | 0 | 0 | 540 | 2000 | 540 | 2000 | Project 2 TMT & Share Point software upgrades |
| Enterprise Database Management | | 0 | 0 | 960 | 2000 | 2000 | 2000 | |
| Enterprise DB upgrades | | 0 | 0 | 540 | 2000 | 2000 | 2000 | |
| Classified Collaboration System | | 0 | 0 | 480 | 480 | 480 | 480 | Workload will go to Enterprise, date to be determined |
| MS Share Point Administration | | 0 | 0 | 480 | 2000 | 2000 | 1000 | |
| Collaboration System Upgrade | | 0 | 0 | 540 | 2000 | 2000 | 2000 | Project 1 to 2 upgrades |
| **ENGINEERING & TIER 3 SERVICES** | | | | | | | | |
| Requirements Analysis | Split among Tier 3 Support | 0 | 2000 | 1000 | 2000 | 2000 | 2000 | |
| System Integration | | 0 | 2000 | 1000 | 2000 | 2000 | 2000 | |
| Enterprise Network Engineering | 3FTE CCIE & Juniper Expert | 0 | 0 | 0 | 6000 | 6000 | 6000 | |
| Enterprise UC engineering | 1.5 FTE CCNP Collaboration | 0 | 1000 | 1000 | 3000 | 3000 | 3000 | |
| Enterprise VDI Engineer | 4 FTE Senior System Admin | 0 | 0 | 2000 | 4000 | 6198 | 7760 | |
| DevSecOps Platform | 1 FTE Senior System Analyst | 0 | 0 | 0 | 0 | 1099 | 1880 | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Enterprise TMT Engineer | .5 FTE System Administrator | 0 | 0 | 500 | 1000 | 1000 | 1000 | |
| Data Center Infrastructure Engineering | 1 FTE CNP Data Center | 0 | 0 | 0 | 2000 | 2000 | 2000 | |
| VM Ware Engineering | 1 FTE w/VM Ware Certs | 0 | 0 | 4000 | 2000 | 2000 | 2000 | |
| System Storage Capacity Management | | 12 | 480 | 480 | 480 | 480 | 480 | |
| Technical Project Management Support | 1 FTE System Engineer/ Analyst | 0 | 2000 | 2000 | 7000 | 6000 | 6000 | |
| Architecture Support | 1 FTE System Analyst | 0 | 0 | 1000 | 1000 | 1000 | 1000 | |
| Mission Relevant Terrain Cyber & Mission Mapping | | 0 | 0 | 1000 | 1000 | 1000 | 1000 | |
| Cyber Security Services (all A6 managed systems) | 2 FTE Cyber Surety Specialist | 0 | 4000 | 4000 | 4000 | 4000 | 4000 | |
| Defensive Cyber Operations | 2 FTE Cyber Security Specialist | 0 | 1700 | 4000 | 4000 | 4000 | 4000 | |
| Network Administrator | 1 FTE Network Engineer | 0 | 0 | 0 | 0 | 0 | 2000 | |
| **BASE COMMUNICATIONS PLANNERS (CP)** | | | | | | | | |
| Ramstein IT CP | 3 PMPs | 0 | 2834 | 4000 | 6000 | 6000 | 6000 | 2 x 86 CS<br>1 x 603 ACOMS |
| Spangdahlem IT CP | 1 PMP | 0 | 2000 | 2000 | 2000 | 2000 | 2000 | |
| Lakenheath IT CP | 2 PMPs | 0 | 0 | 0 | 4000 | 4000 | 4000 | |
| Molesworth IT CP | 1 PMP | 0 | 2000 | 2000 | 2000 | 2000 | 2000 | 502 CSW |
| RAF Fairford IT CP | 1 PMP | 0 | 2000 | 2000 | 2000 | 2000 | 2000 | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Aviano IT CP | 1 PMP | 0 | 2000 | 2000 | 2000 | 2000 | 2000 | |
| Incirlik IT CP | 1 PMP | 0 | 2000 | 2000 | 2000 | 2000 | 2000 | |

## APPENDIX D: USAFE ADDITONAL NONDISCLOSURE AGREEMENT FOR CONTRACTOR EMPLOYEES

(SS#:5, RR#: A076)

I, ___________________________(print or type name), as an employee of ______________________ (insert name of company), a contractor hired under contract number:___________________(insert number), Task Order#: ________________(insert number) pursuant to support HQ USAFE-AFAFRICA Communication Directorate, agree not to disclose to any individual business entity or anyone within ____________________ (insert name of employee company and/or sub-contractor) or outside the company who has not signed a nondisclosure agreement for the purposes of performing under this contract. Any sensitive, proprietary or source selection information contained in or accessible through the ________________(insert contract name) project. Proprietary information/data will be handled IAW Government regulations.

I understand that information/data I may be aware of, or possess, as a result of my assignment under this contract may be considered sensitive or proprietary by HQ USAFE/AFAFRICA. The contractor's responsibility for proper use and protection from unauthorized disclosure of sensitive, proprietary and source selection information is described in Federal Acquisition Regulation (FAR) section 3.104-5(b). Pursuant to FAR 3.104-5, I agree not to appropriate such information for my own use or to release or discuss such information for my own use or to release it to or discuss it with third parties unless specifically authorized in writing to do so, as provided above.

This agreement shall continue for a term of 5 years from the date upon which I last have access to the information there from. Upon expiration of this agreement, I have a continuing obligation not to disclose sensitive, proprietary, or source selection information to any person or legal entity unless that person or legal entity is authorized by the head of the agency or the contracting agency or the contracting officer to receive such information. I understand violations of this agreement are subject to administrative, civil and criminal sanctions.

THIS CERTIFICATION CONCERNS A MATTER WITHIN THE JURISDICTION OF AN AGENCY OF THE UNITED STATES AND THE MAKING OF A FALSE, FICTITIOUS, OR FRAUDULENT CERTIFICATION MAY RENDER THE MAKER SUBJECT TO PROSECUTION UNDER TITLE 18, UNITED STATES CODE, SECTION 1001.

___________________________________ ___________________________________
(Signature of Contractor Employee) Date

___________________________________ ___________________________________
(Signature of KTR representative and title) Date

___________________________________ ___________________________________
Signature of COR Date

# APPENDIX E: HARDWARE AND SOFTWARE OVERVIEW.

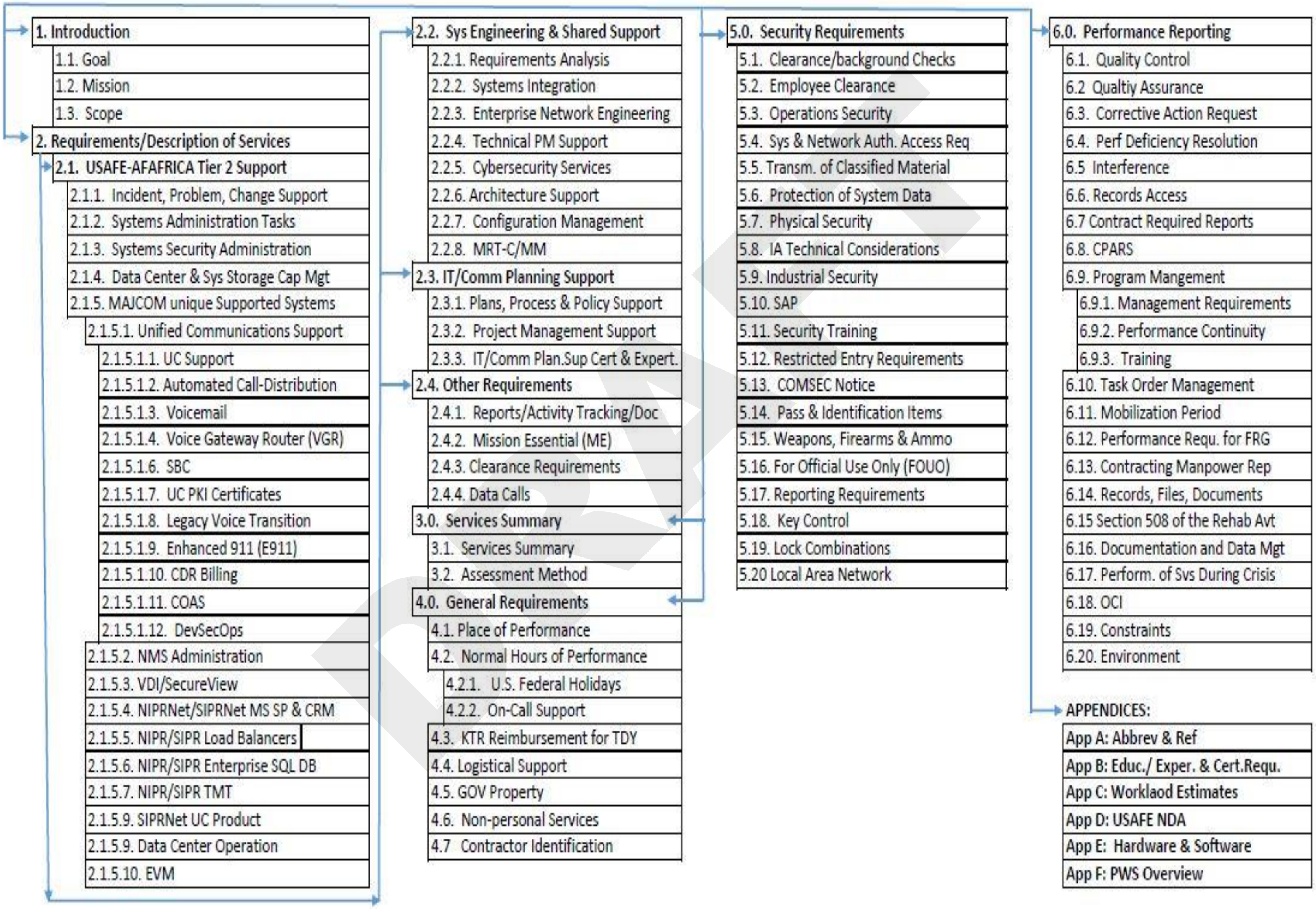
**E.1.** The following list is the hardware and software currently deployed to date in the USAFE Theater Storage and Virtualization Infrastructures. The intent of this list is solely to provide the KTR a rough overview of the current infrastructure hardware and software. This is not an all-inclusive list nor a list of Government Furnished Equipment (GFE), and the KTR will not be assigned as the custodian of this equipment.

| **USAFE Theater Data Center Hardware and Software** | **Manufacturer** |
|---|---|
| EMC CLARiiON AX/CX/NX Series | EMC |
| Navisphere | EMC |
| Unisphere | EMC |
| MirrorView | EMC |
| EMC DMX | EMC |
| EMC Symmetrix 8xxx | EMC |
| Symmetrix Management Console | EMC |
| EMC Celerra CNS, CFS, NS40g, NSX, G48 | EMC |
| Celerra Manager | EMC |
| NAS Command Line 5.5.x, 5.6.x | EMC |
| Brocade Fibre Switches DS-300B | Brocade |
| Fabric Manager | Brocade |
| Cisco Fibre Switches MDS 9xxx | Cisco |
| Cisco Application Policy Infrastructure Controller (Cisco APIC) | Cisco |
| Cisco Nexus Data Center Switches 5000 and 9000 series | Cisco |
| Device Manager and Fabric manager | Cisco |
| ESX, ESXi 5.0, 5.5, 6.x | VMware |
| Storage vMotion | VMware |
| DRS / HA | VMware |
| Stage / Lab Manager | VMware |
| Site Recovery Manager | VMware |
| vCenter 4.0, 5.0, 5.5 | VMware |
| EMC Centera Gen 4LP | EMC |
| Avamar Gen 2 | EMC |
| Power Path Current Version | EMC |
| EMC ControlCenter 6.x | EMC |
| CommVault Galaxy and Simpana | CommVault |
| StorageScope File Level Reporter | EMC |
| Rainfinity | EMC |
| Data Protection Advisor (DPA) | EMC |
| SRDF | EMC |
| Recover Point 3.2 | EMC |
| Backup Exec 11d & 12.5 | Symantec |
| Data Domain 140, 620, 640, 670, 690 860, 890 | EMC |
| EMC VNXe 3100 and 3300; VNX 5500 and 7500 | EMC |
| VMWare Horizon | VMWare |
| VMWare ThinApp | VMWare |
| VMWare vShield Endpoint 5 | VMWare |
| Cisco VXc Client Manager | Cisco |
| **VDI/SecureView Hardware and Software** | **Manufacturer** |

| | |
|---|---|
| Cisco Unified Computing System (UCS) host servers | Cisco |
| Cisco Firepower 4000 series (VPN, FW, IPS) | Cisco |
| Cisco layer 3 switches | Cisco |
| WYSE Thin Clients / Zero Clients | Dell |
| Dell host servers | Dell |
| SecureView workstations | HP |
| Windows Server | Microsoft |
| SQL Server | Microsoft |
| EXSi, VSphere, vCenter | VMWare |
| vCenter Operations Manager for Horizon | VM Ware |
| Horizon View Suite | VM Ware |
| Thin App | VM Ware |
| SecureView Management Server (SVMS) | AFRL |
| LogRhythm XM SIEM Appliance | LogRhythm |
| ISC CertAgent | ISC |
| Aruba VPN | Aruba |

# APPENDIX F:  PWS Overview

# INFORMATION TECHNOLOGY SUPPORT SERVICES



- 1. Introduction
  - 1.1. Goal
  - 1.2. Mission
  - 1.3. Scope
- 2. Requirements/Description of Services
  - 2.1. USAFE-AFAFRICA Tier 2 Support
    - 2.1.1. Incident, Problem, Change Support
    - 2.1.2. Systems Administration Tasks
    - 2.1.3. Systems Security Administration
    - 2.1.4. Data Center & Sys Storage Cap Mgt
    - 2.1.5. MAJCOM unique Supported Systems
      - 2.1.5.1. Unified Communications Support
        - 2.1.5.1.1. UC Support
        - 2.1.5.1.2. Automated Call-Distribution
        - 2.1.5.1.3. Voicemail
        - 2.1.5.1.4. Voice Gateway Router (VGR)
        - 2.1.5.1.6. SBC
        - 2.1.5.1.7. UC PKI Certificates
        - 2.1.5.1.8. Legacy Voice Transition
        - 2.1.5.1.9. Enhanced 911 (E911)
        - 2.1.5.1.10. CDR Billing
        - 2.1.5.1.11. COAS
        - 2.1.5.1.12. DevSecOps
      - 2.1.5.2. NMS Administration
      - 2.1.5.3. VDI/SecureView
      - 2.1.5.4. NIPRNet/SIPRNet MS SP & CRM
      - 2.1.5.5. NIPR/SIPR Load Balancers
      - 2.1.5.6. NIPR/SIPR Enterprise SQL DB
      - 2.1.5.7. NIPR/SIPR TMT
      - 2.1.5.9. SIPRNet UC Product
      - 2.1.5.9. Data Center Operation
      - 2.1.5.10. EVM
  - 2.2. Sys Engineering & Shared Support
    - 2.2.1. Requirements Analysis
    - 2.2.2. Systems Integration
    - 2.2.3. Enterprise Network Engineering
    - 2.2.4. Technical PM Support
    - 2.2.5. Cybersecurity Services
    - 2.2.6. Architecture Support
    - 2.2.7. Configuration Management
    - 2.2.8. MRT-C/MM
  - 2.3. IT/Comm Planning Support
    - 2.3.1. Plans, Process & Policy Support
    - 2.3.2. Project Management Support
    - 2.3.3. IT/Comm Plan.Sup Cert & Expert.
  - 2.4. Other Requirements
    - 2.4.1. Reports/Activity Tracking/Doc
    - 2.4.2. Mission Essential (ME)
    - 2.4.3. Clearance Requirements
    - 2.4.4. Data Calls
- 3.0. Services Summary
  - 3.1. Services Summary
  - 3.2. Assessment Method
- 4.0. General Requirements
  - 4.1. Place of Performance
  - 4.2. Normal Hours of Performance
    - 4.2.1. U.S. Federal Holidays
    - 4.2.2. On-Call Support
  - 4.3. KTR Reimbursement for TDY
  - 4.4. Logistical Support
  - 4.5. GOV Property
  - 4.6. Non-personal Services
  - 4.7 Contractor Identification
- 5.0. Security Requirements
  - 5.1. Clearance/background Checks
  - 5.2. Employee Clearance
  - 5.3. Operations Security
  - 5.4. Sys & Network Auth. Access Req
  - 5.5. Transm. of Classified Material
  - 5.6. Protection of System Data
  - 5.7. Physical Security
  - 5.8. IA Technical Considerations
  - 5.9. Industrial Security
  - 5.10. SAP
  - 5.11. Security Training
  - 5.12. Restricted Entry Requirements
  - 5.13. COMSEC Notice
  - 5.14. Pass & Identification Items
  - 5.15. Weapons, Firearms & Ammo
  - 5.16. For Official Use Only (FOUO)
  - 5.17. Reporting Requirements
  - 5.18. Key Control
  - 5.19. Lock Combinations
  - 5.20 Local Area Network
- 6.0. Performance Reporting
  - 6.1. Quality Control
  - 6.2 Qualtiy Assurance
  - 6.3. Corrective Action Request
  - 6.4. Perf Deficiency Resolution
  - 6.5 Interference
  - 6.6. Records Access
  - 6.7 Contract Required Reports
  - 6.8. CPARS
  - 6.9. Program Mangement
    - 6.9.1. Management Requirements
    - 6.9.2. Performance Continuity
    - 6.9.3. Training
  - 6.10. Task Order Management
  - 6.11. Mobilization Period
  - 6.12. Performance Requ. for FRG
  - 6.13. Contracting Manpower Rep
  - 6.14. Records, Files, Documents
  - 6.15 Section 508 of the Rehab Avt
  - 6.16. Documentation and Data Mgt
  - 6.17. Perform. of Svs During Crisis
  - 6.18. OCI
  - 6.19. Constraints
  - 6.20. Environment
- APPENDICES:
  - App A: Abbrev & Ref
  - App B: Educ./ Exper. & Cert.Requ.
  - App C: Worklaod Estimates
  - App D: USAFE NDA
  - App E: Hardware & Software
  - App F: PWS Overview