PERFORMANCE WORK STATEMENT (PWS)

for

AIR FORCE RESERVE COMMAND

AFRC Enterprise IT Services

9 March 2017

Description of Services

1.1. **Background/Scope**:

HQ AFRC/A6 requires contractor services in support of the planning, analysis, operation, management, administration, user support, and cyber work force development for the information technology environment of the Air Force Reserve Command (AFRC).

AFRC encompasses HQ AFRC, AFRC host bases, non-AFRC tenants, and AFRC tenants. Terms are as follows:

The term 'HQ AFRC' applies to all AFRC personnel, facilities, and equipment located at Robins AFB, GA. Currently, HQ AFRC is spread across nine (9) buildings. During this contract period, HQ AFRC will move to a Consolidated Mission Complex (CMC) that will house all of HQ AFRC in fewer, co-located buildings. This will require additional efforts to move and support a transitioning user base to the final, physical configuration.

The term 'AFRC Host Base' applies to ARPC (Buckley), Dobbins, Grissom, Homestead March, Minneapolis-St Paul, NAS-JRB Ft Worth (Carswell), Niagara Falls, Pittsburgh, Westover, and Youngstown where all communications support is provided by AFRC.

The term 'non-AFRC tenant' applies to tenants on AFRC Host Bases receiving AFRC communications support.

The term 'AFRC tenant' applies to all AFRC units not physically located on an AFRC Host Base.
All references to 'day' means calendar day unless otherwise specified.

Scope includes Information Technology (IT) services for the Non-Secure Internet Protocol Router (NIPR) Network, the Secure Internet Protocol Router (SIPR) Network, Program/Project Management; Enterprise Architecture (EA); spectrum management, and related support services as described below.

2. PROGRAM MANAGEMENT, ANALYSIS, AND SUBJECT MATTER EXPERT (SME) SUPPORT. AFRC/A6 is responsible for planning, analyzing, and managing Enterprise-wide projects and programs, enterprise architecture, and spectrum, as well as providing administrative functions for IT equipment accountability, package delivery, and cyber force development as described in paragraphs 2.1. through 2.13.

2.1. **Enterprise IT Services General Support– (A6X)**. HQ AFRC requires full-time Program Management (PM) to be co-located with AFRC/A6 in order to facilitate Government-Contractor communications and fulfill the overall performance of this contract.

2.1.1. Contractor shall ensure the following tasks are accomplished:

- Provide on-site, full-time program management support at HQ AFRC to facilitate Government-Contractor communications.
- Supervise contractor personnel at multiple geographical locations (see Table 3).
- Responsible for daily administration of the contract including, but not limited to, duty assignment for all contract personnel (whether prime or subcontractor).
- Responsible for formulating and enforcing work standards, assigning schedules, reviewing work discrepancies, and communicating policies, objectives, and goals of the organization to subordinates.
- Maintain satisfactory contract performance and resolve issues timely.
- Notify the COR prior to implementing actions that will impact services' deliveries.
- Meet project schedule milestones on-time delivery at or above 90% level. Late deliveries must not be more than 5 days late.
- Provide accurate/comprehensive MTS, MFS, MPS, MKPS, and Monthly Metrics reports within 10 work days after end of month with on-time delivery at 100% level.
- Meet with the COR, as needed, to maintain satisfactory performance and to resolve issues pertaining to Government-Contractor procedures.
- Ensure written minutes are prepared for meetings.
- Ensure support is provided to all other meetings, working groups, etc.
- Establish and maintain a metrics program to document, trend, perform analyses, and brief its performance to the Government. The Government will validate the metrics for acceptance. Any discrepancies to the metrics will be returned to the Contractor for correction and re-submitted to the Government for acceptance within 5 business days.
- Ensure all contractor trip reports (for any travel performed in support of the contract) are submitted within 5 business days of completion of the trip. This report shall be electronically delivered to the COR via email.
- Identify and report all program management actions in a Monthly Technical Summary (MTS) Report and/or as requested by the Government. This report shall be electronically delivered to the COR via email and contain the following information:
    - Brief description of requirements.
    - Brief summary of accomplishments during the reporting period and significant events regarding the contract.
    - Any current or anticipated problems and the resolution.
    - Summary of all major events and other pertinent information.
    - Technical user support activity summary.
    - Summary of associated travel completed.
    - Summary of planned travel.
    - Brief summary of activity planned for the next reporting period.
    - Task schedules/work plans.
    - Task performance metrics.
    - Task software quality metrics.

- Identify and report project summaries in a Monthly Key Project Status (MKPS) Report. Key projects will be designated by the Government. This report shall be electronically delivered to the COR via email and contain the following information:
  - Compliance to individual project schedule milestones as jointly agreed between Government and Contract Program Manager as demonstrated by:
    - Milestone charts (e.g., Gantt chart)
    - Overall schedule status (e.g., on schedule, behind schedule, limiting factors)
    - Percentage of completion
    - Narrative project synopsis
      - Phase of project
      - Identification of any problems, issues or delays
      - Recommendations
      - Corrective actions
- Identify and report financial management status in a Monthly Financial Summary (MFS) Report. This report shall be electronically delivered to the COR via email and contain the following information:
  - Billing summary for reimbursable costs [broken out for labor, training, travel, other direct costs (ODC)] during the reporting period.
  - Vendor Labor Hour Expense/Burn Rates for reimbursable costs.
- Identify and report in a Monthly Metrics Report, metrics to include:
  - Cyber Development Metrics (2.13.1., 2.13.4.)
  - Virtual Environments capacity, performance and utilization Metrics (3.4.3.4.)
  - WAN bandwidth utilization and latency metrics (3.4.6.1.4.)
  - Vulnerability metrics for assigned servers and workstations (3.4.1., 3.5.1.1., 3.7.1., 3.7.2.1., 3.7.3.1., 3.8.1.1., 4.27.2.)
  - Blackberry/Good license usage metrics (3.4.7.4.)
  - Storage and backup environments capacity, performance and utilization metrics (3.4.9.4.)
  - Servers, print devices, and utilization rates metrics (3.4.14.4.)
  - PKI/LRA Token Metrics (3.4.15.4.)
  - Database accuracy metrics (3.4.16.4.)
  - SharePoint environments capacity, performance, uptime, and utilization Metrics (3.4.17.2.4.)
  - Server, workstation, and infrastructure vulnerability metrics (3.5.1.4.)
  - CFP Ticket Performance Metrics (3.7.1.4., 3.7.2.4., 4.27.2.)
  - VTC Usage Metrics with a 99% success rate of VTC sessions per month (3.8.1.4., 4.27.2.)
  - Data accuracy metrics (3.8.5.2.4.)
  - SOCE health metrics (3.8.5.3.4.)
  - SOCE service availability metrics (3.8.5.3.4.)
- Complete and maintain a Monthly Personnel Summary (MPS) Report, based on the Government provided spreadsheet. Information to include:

- All tasks identified on the contract, reference by paragraph
- Name of contractor assigned to each task
- Location where task is being performed
- Contractor start date
- 8570 position number contractor assigned to
- Type of 8570 requirements/Type of Certification
- Tracks 8570 training requirements
- Non-Disclosure Agreement (NDA)
- Privileged Access Agreement (PAA)

2.1.2. Qualifications:

- Experience as a PM performing duties on an IT contract of similar size, scope, and complexity.
- Significant program management experience including supervising/managing a large IT workforce.
- Experience with liaison activity associated with various levels of management within DoD, or equivalent, including contracts.
- Experience in personnel management, strategic planning, risk management, change management.
- Experience performing mathematical and analytical functions required to capture and produce meaningful metrics.
- Technical IT knowledge regarding computers, systems, databases, and general use software programs.

2.1.3. Certifications:

- None required.

2.1.4. Deliverables:

- Monthly Technical Summary (MTS) Report. **(CDRL A001)**
- Monthly Financial Summary (MFS) Report. **(CDRL A002)**
- Monthly Key Project Status (MKPS) Report. **(CDRL A031)**
- Monthly Personnel Summary (MPS) Report. **(CDRL A004)**
- Monthly Metrics Report. **(CDRL A003)**
- Meeting minutes. (**CDRL A005)**

2.2. Project Management Support (A6XP). All project management functions listed in para 2.3. through 2.8. will include the following requirements in addition to what is identified in those sections:

2.2.1. Contractor shall ensure the following tasks are accomplished::

- Conduct technical research on possible solutions.
- Plan training, equipment deployment, installation, technical support, engineering and sustainment to AFRC for assigned programs.

- Provide cost estimates, evaluation of proposed solutions, and implementation plans for AFRC.
- Assist AFRC in troubleshooting program issues.
- Track and manage responses from Point of Contacts (POCs) across AFRC to meet suspenses.
- Ensure project conformance with AFRC, Air Force (AF) and DoD guidance.
- Assist HQ AFRC Information Systems Security Manager (ISSM) with IA and C&A requirements, as required.

2.2.2. Qualifications:
- Significant experience in IT project management.
- Proficient in MS Office tools, including MS Project.

2.2.3. Certifications:
- See specific certification requirements in paragraphs 2.3.3, 2.4.3., 2.5.3., 2.6.3., 2.7.3., and 2.8.3.

2.2.4. Deliverables:
- Program portfolios **(CDRL A006)** for each program, which include:
  - Meeting minutes
  - POCs
  - Project status slides
  - Program Management Reviews (PMRs)
  - Timelines and milestones for each assigned project
  - Weekly briefings or written reports on assigned projects.
  - Technical solutions
  - Engineering and installation drawings
  - Site survey reports.
  - Lifecycle management plan.
  - Projects will have a portfolio established within 30 days of assignment; reviewed weekly to incorporate changes.

2.3. <u>Unified Capability (UC) Support – (A6XP)</u>. Unified Capability enables strategic, tactical, classified, and multinational missions with a broad range of interoperable and secure capabilities for converged non-assured and assured voice, video, and data services from the end device, through Local Area Networks (LANs), and across the backbone networks. AFRC is expected to complete the transition to a 100% Voice Over Internet Protocol (VoIP) solution at nine (9) AFRC host bases by September 2018. In addition, the AF is planning to combine multiple platforms into one communications solution, merging Cisco voice capabilities with instant messaging, mobile and soft phone applications throughout AFRC.

2.3.1. Contractor shall ensure the following tasks are accomplished:
- Refer to para 2.2.1.

- Develop technical solutions.
- Create network and engineering diagrams.
- Process formal UC waivers through HQ AF.
- Manage projects to include:
  - Transition of AFRC UC solutions to Joint Information Environment (JIE).
  - Implementation of Defense Information Systems Agency (DISA) Session Initiation Protocol (SIP) Trunking, when available.
  - AFRC/AF Enterprise implementation of VoIP transition.
  - AFRC enterprise mobile UC capabilities

2.3.2. Qualifications:

- Refer to para 2.2.2.
- Significant experience administering or designing Cisco UC systems including Cisco Unified Communications Manager.
- Experience deploying SIP trunking.
- Experience integrating with 3rd party communications solutions (e.g., MS Lync, Skype for Business).
- Experience migrating legacy PBX infrastructure to unified communications.
- Experience with multi-site, IP telephony and unified communications rollouts/migrations.

2.3.3. Certifications:

Cisco Certified Associate Level (e.g., CCNA) certification or Cisco Certified Professional Level (e.g., CCNP) certification required.

2.3.4. Deliverables:

- Refer to para 2.2.4.

2.4. <u>MAJCOM Information Management and Data Visualization Support – (A6XP)</u>.

2.4.1. Contractor shall ensure the following tasks are accomplished:

- Refer to para 2.2.1.
- Train and troubleshoot with stakeholders to ensure adherence to established business rules.
- Create and maintain user guides and business rules IAW the applicable governing board.
- Create and maintain SharePoint sites, as required.
- Responsible for oversight of any Personally Identifiable Information (PII) issues and proper protection of FOUO data and classified data
- Coordinate ICM tool upgrades/changes.
- Market capabilities and seek new user base for Enterprise Calendar (EC) content.
- Coordinate Major Command (MAJCOM) EC content and maintain status.
- Validate content and currency of MAJCOM EC.

- Manage the AFV programs and support additional initiatives for data visualization using geospatial and/or dashboarding tools.

2.4.2. Qualifications:
- Refer to para 2.2.2.
- Experience administering SharePoint site.
- Knowledge of data visualization, geospatial and/or dashboarding tools.

2.4.3. Certifications:
- None required.

2.4.4. Deliverables:
- Refer to para 2.2.4.

2.5. Mobile and Communications Initiatives Support – (A6XP). Mobile initiative support involves Enterprise Mobility Management for Apple iOS, Android, and Window devices to include Mobile Device Management (MDM) and Mobile App Management (MAM) Mobile Content Management (MCM). AFRC will also often create a pilot project to explore a new technology. Additionally, HQ AF or Program Management Offices (PMOs) will dictate new initiatives or upgrade plans for AFRC.

2.5.1. Contractor shall ensure the following tasks are accomplished:
- Refer to para 2.2.1.
- Provide program management of Mobile initiatives [e.g., Mobile Mission Kits (MMK), Electronic Flight Bag (EFB), e-Tools]
- Manage projects that include, but are not limited to:
  - Internal Mass Notification System (IMNS) over VoIP
  - Security camera video feeds (Closed Circuit TV) over Internet Protocol (IP)
  - Communication requirements for HQ AFRC building moves
  - Communication requirements for AFRC MILCON projects
  - AFRC's cryptographic modernization project
  - Installation of Global Aircrew Strategic Network Terminals (ASNTs)

2.5.2. Qualifications:
- Refer to para 2.2.2.

2.5.3. Certifications:
- None required.

2.5.4. Deliverables:
- Refer to para 2.2.4.

2.6. Video Teleconferencing (VTC) and Audio/Visual (A/V) Support – (A6XP). AFRC manages 74 Secure or Non-Secure IP VTC systems across the enterprise. In

addition, AFRC designs and maintains VTC and A/V capability for 8 suites at HQ AFRC.

2.6.1. Contractor shall ensure the following tasks are accomplished:

- Refer to para 2.2.1.
- Maintain information from each site including equipment lists, drawings and testing/certification data.
- Develop technical solutions.
- Create network and engineering diagrams.
- Make recommendations to leadership on new VTC and Audio/Visual (A/V) capabilities.
- Serve as the VTC configuration manager and facilitator for HQ AFRC.
- Maintain VTC Account Database utilizing Telepresence Management Suite.
- Track, document and brief management on VTC utilization trends.
- Maintain awareness of fielded inventory equipment.
- Conduct sites surveys; assess and document current site configuration and user requirements.
- Assist VTC System Engineering Support (para 3.8.3.1.) with technical tasks, as required.
- Provide VTC Usage Metrics with a 99% success rate of VTC sessions per month.

2.6.2. Qualifications:

- Refer to para 2.2.2.
- Significant experience administering and configuring VTCs and A/V suites.
- Experience integrating VTCs and A/V equipment with 3rd party communications solutions.
- Experience with Crestron products, integration, and programming.
- Knowledge of various A/V technologies.
- Knowledge of VTC technologies and common architecture equipment (e.g., Cisco, Codian).
- Knowledge of AF network architecture and security, including:
  - Authority to Operate (ATO) changes and considerations
  - Joint Interoperability Test Command (JITC) certifications
  - Approved Product List (APL) / UC
  - TEMPEST and EMSEC standards
  - Crestron products, integration, and programming
- Experience with multicast on desktops (streaming audio/video), audio conferencing, point-to-point, and multipoint video conferencing.

2.6.3. Certifications:

- Cisco Certified Associate Level (e.g., CCNA) or CCNA-Collaboration certification required.

2.6.4. Deliverables:

- Refer to para 2.2.4.
- Status reports of task activities, as required. **(CDRL A009)**
- New technology research briefings/reports, as required. **(CDRL A011)**
- Trend and performance analysis reports. **(CDRL A010)**

2.7. Enterprise Network Infrastructure Support – (A6XP). AFRC manages network infrastructure for HQ AFRC and AFRC host bases. Additionally, AFRC is testing new mediums for network infrastructure including cellular and wireless systems. Further, enterprise-wide configuration management and inventory are located at HQ AFRC.

2.7.1. Contractor shall ensure the following tasks are accomplished:
- Refer to para 2.2.1.
- Projects include, but are not limited to:
  - Coordinate and develop new infrastructure solutions including cellular and wireless systems
  - Identify and maintain an inventory of enterprise network devices
  - Determine future datacenter infrastructure based on AF functional specifications and Data Center Optimization Initiative (DCOI)
- Develop technical solutions.
- Create network and engineering diagrams.
- Make recommendations to leadership on new infrastructure technologies/capabilities.
- Evaluate inventory of enterprise network devices.
- Oversee AFRC infrastructure configuration management.
- Assist Network Infrastructure Engineering Support (para 3.4.11).

2.7.2. Qualifications:
- Refer to para 2.2.2.
- Significant experience administering or configuring Cisco based network infrastructure.
- Knowledge of configuring or designing enterprise wireless networks.

2.7.3. Certifications:
- Cisco Certified Associate Level (e.g., CCNA) certification or Cisco Certified Professional Level (e.g., CCNP) certification required.

2.7.4. Deliverables:
- Refer to para 2.2.4.

2.8. Data Center Optimization Initiative (DCOI) Support – (A6XP). AFRC manages enterprise services for HQ AFRC and AFRC Host Bases. Federal guidance requires agencies to develop and report on data center strategies to consolidate inefficient infrastructure, optimize existing facilities, improve security posture, achieve cost savings,

and transition to more efficient infrastructure, such as cloud services and inter-agency shared services. Further guidance will be provided by DoD and HQ AF.

2.8.1. Contractor shall ensure the following tasks are accomplished:

- Refer to para 2.2.1.
- Projects include, but are not limited to:
  - Develop cloud transition plan for AFRC enterprise applications (Mil Cloud and/or Commercial Cloud).
  - Transition AFRC Installation Processing Nodes (IPNs) to conform to AF functional specifications.
- Manage application rationalization listing for AFRC.
- Process enterprise-wide data center spend plans and Data Center Obligation Requests (DCORs).
- Manage MAJCOM Datacenter Inventory Management (DCIM) tool.

2.8.2. Qualifications:

- Refer to para 2.2.2.
- Knowledge of Virtualization.
- Knowledge of Cloud Services specifically Infrastructure as a Service (IaaS).

2.8.3. Certifications:

- None required.

2.8.4. Deliverables:

- Refer to para 2.2.4.

2.9. <u>Enterprise Architecture (EA) Program Support</u>. The objective of this effort is to obtain Enterprise Architecture (EA) services to enhance and manage Air Force Reserve Command (AFRC) EA capabilities. This requirement includes the solutions that integrate existing and evolving governance, EA tools, frameworks, methodologies, models, and artifacts with the goals to use EA to eliminate redundancy, build efficiency, and optimize utilization of resources. AFRC EA structure currently includes the requirement herein, a Government Chief Enterprise Architect (CEA) at HQ AFRC, two (2) Government EA positions within HQ AFRC/A6XC, a separately contracted EA strategic support team spread across three (3) AFRC locations, and stakeholders ranging from the executive management level to system owners and users. The Contractor shall ensure support of the EA strategic, operational, and solution level goals and efforts of the AFRC CEA, AFRC EA Government lead, and AFRC Chief Information Officer (CIO) branch. The AFRC CEA is the AFRC approval authority for all AFRC EA artifacts. The scope of EA services and support will be associated with all IT business investments made by and on behalf of AFRC. These services include EA design and review, governance support, EA technical writing and documentation, and EA software support.

2.9.1. <u>Enterprise Architecture Support – (A6XC)</u>. Enterprise architects are required for EA design, review, governance support, technical writing, and documentation. AFR utilizes architecture products at all organizational levels to help managers and decision makers achieve maximum effectiveness, efficiency, and economies of scale from IM/IT investments. Architectures enhance collaboration with executives, managers, staff, authorized contractors, and any other AFRC stakeholder, within, and external to AFRC (stakeholders and partners), who impact the design of AFRC enterprise. There are approximately 200 existing artifacts to be maintained, with new artifacts continually required to support additional new projects.

2.9.1.1. **Contractor shall ensure the following tasks are accomplished:**

- Produce and/or collaborate with other Government entities to create EA graphical views ("artifacts") for existing or new systems/applications, business processes, and/or data**.**
  - Generate the architectural artifacts using the Government specified tool, currently IBM Rational System Architect and IBM InfoSphere Data Governance.
  - Design, create, and provide quality assurance on architecture products IAW latest version of DoDAF and subsequent revisions, DOD, AF, and AFR EA standards; the latest version of DoDAF and BEA standards are to be implemented upon official release for use.
  - Develop DoDAF artifacts for the Government program manager submission to the Business EA (BEA) tool as defined in the DoD BEA.
  - Develop DoDAF artifacts to support National Defense Authorization Act (NDAA) requirements.
  - Develop and maintain architecture products to include data models, system architectural and interface products, and process models.
  - Review architectures for AFR EA Modeling Standards compliance.
  - Follow AFRC internal architecture governance processes for architecture approvals.
  - Design/create target (To-Be) architectures to address capability gaps found during analysis; provides written recommended steps needed to transition to "to be" state, when required.
- Provide support that ensures the AFRC EA is federated to AF EAs.
  - Deliver AFRC Segment architectures with goal of federating AFRC architecture with AF and AF Domain EA(s).
- Conduct enterprise-wide and cross-domain data and architectural analyses and review; emphasis on promoting system convergence and investment optimization.
- Develop and maintain a business catalog that describes AFRC data needs; a single vocabulary referencing all of AFRC data as agreed upon by AFRC organizations.
- Promote service oriented architecture (SOA) approaches to solutions; develop service architectures to replace legacy environments and implements new capabilities.

- Develop, maintain, and utilize the Service Development and Delivery Process (SDDP) to analyze and support new IT requirements.
  - Monitor the progress of assigned IT requirements until a solution is implemented, inform the customer and AFRC leadership of status updates, and provide cross-functional AFRC project support.
  - Assist/facilitate requirement owners with delivery of SDDP Step 1 and 2 products to include Performance Reference Models (PRM) and Business Reference Models (BRM).
  - Aid in the identification of potential duplicate capabilities or existing re-useable capabilities.
  - Assist/facilitate and perform business analysis for requirement owners through delivery of some SDDP Step 3 products; to include multiple solution courses of action (COAs), obtaining information by reaching out to other Government agencies as needed for cost and schedule estimates.
  - Develop artifacts to support the bounded user requirements. Minimum list of artifacts to support the bounded user requirements include, but are not limited to: AV-1, CV-2, OV-1, OV-5b BPMN, OV-6c BPMN, SV-1, DIV-1, DIV-2, StdV-1, and SvcV-1 (SvcV-1, as needed, for service related requirements). This is the minimum acceptable architecture that must be delivered, but is not to be interpreted as a complete list of architectural artifacts that may be required for a requirement.
- Design and develop SDDP communication products.
- Create architecture decision support reports showing overlapping or duplicate capabilities and recommends system/application transition, consolidation, and sun-setting actions.
- Assist/gather/provide architecture information for Analysis of Alternatives (AoA).
- Provide training on EA services, processes, tools and methodologies to stakeholders and partners.
- Attend applicable AF Communities of Interest (COIs) or other architecture-impacting groups.
- Collaborate horizontally and vertically across multiple organizations to support AFRC's involvement in IT transformation initiatives.
- Identify and evaluate AFRC applicability of DoD and AF architecture strategies, guidance, and policies to ensure AFRC compliance with higher-level architecture processes and procedures.
- Develop templates to support appropriate document generation standards and manage the versions; generate interactive (html) version and other MS-Office managed versions.
- Ensure compliance with, and collaborate on updates/changes to, AFR EA guidance and documentation. (Note: EA guidance currently consists of AFR EA Charter, AFR EA Processes & Procedures Guide, AFR EA Modeling Standards, AFR EA Approval & Certification Process Guide, AFR Service Development and Delivery Guidebook, AFR Maturity Assessment, AFR Future State, and AFR EA Skills and Training Guide.)

- Review and update published material such as the EA AFR Processes and Procedures document, AFR EA SDDP Guide, AFR EA Charter, and AFR EA Modeling Standards document, as designated by the Government; recommend revisions or changes in scope, format and content.
- Develop or maintain a "Fit for Purpose" architecture compliance requirements checklist, to be used in the Government architecture approval process.
- Develop and maintain agendas and minutes for EA meetings.
- Develop and maintain EA performance metric statistics and briefings, as required, by AFRC EA Program Management.
- Create/update/maintain AFRC Business, Information, and/or Technical Reference Models.
- Collaborate with the AFRC CEA and AFRC Government EA Lead (or designated representative) to devise and document an AFRC "to be" business, information and technology EA strategy/vision.
- Assist the AFRC CEA office's integration efforts for all EA-related planning, management, investment, evaluation, and revalidation efforts to meet AFRC's operational and business objectives.
- Develop, maintain, and adhere to the EA Annual Operating Plan, including the EA Integrated Master Schedule (IMS). The EA Annual Operating Plan shall be based on EA program guidance and strategy AFRC Government personnel will deliver to the Contractor via an AFR EA Annual Program Plan. The EA Annual Operating Plan components shall include, but are not limited to, the following:
  - A plan describing the Contractor's overall management strategies, policies, procedures, and suggested metrics for all major EA projects and initiatives called out in the AFR EA Annual Program Plan.
  - An IMS, similar to a MS Project/Gantt chart format, to include all projects specified in the EA Annual Operating Plan.
    - IMS shall include dates of major milestones, percent completion status, and identified schedule dependencies.
    - IMS shall be posted in a common electronic area designated by the Government for review (SharePoint or Shared Drive access).
    - IMS shall be updated throughout the year as progress is made on projects.
    - IMS milestone changes shall be coordinated with and approved by the Government.
- Manage, track, evaluate, and provide status updates on project progress and overall EA program health.

2.9.1.2. Qualifications:

- Significant experience creating enterprise architecture in the Department of Defense Architecture Framework (DODAF), Federal Enterprise Architecture Framework (FEAF), Ministry of Defense Architecture Framework (MODAF), or The Open Group Architecture Framework (TOGAF)
  OR
  work experience creating enterprise architecture in either the DODAF, FEAF,

MODAF, or TOGAF and has an enterprise architecture certification, such as a Certified Enterprise Architect (CEA).
- Knowledge of Rational System Architect.
- Proficient in MS Office tools, including MS Project and Visio.
- Trained in the latest version of DODAF (current version is DODAF 2.0).

2.9.1.3. Certifications:
- None required.

2.9.1.4. Deliverables:
- EA Annual Operating Plan with EA Integrated Master Schedule (IMS) within 60 days of Government delivery of AFR EA Annual Plan; with quarterly updates due the 1st work day of each quarter thereafter with an on-time delivery at 100%. **(CDRL A007)**
- Meets scheduled milestones identified in Annual Operating Plan and IMS, as approved by Government with an on-time delivery at 95%. Late deliveries must not be more than 5 days late. **(CDRL A007)**

2.9.2. <u>EA System Administration - (A6XC)</u>. The expected EA technical environment consists of 5 virtual servers, 10-12 clients utilizing VMWare VDI and browser-based access, a primarily Structured Query Language (SQL)-based data repository (with occasional Oracle data analysis required), and support tools that include 10 user licenses for Rational System Architect and IBM InfoSphere Data Governance. Specific EA tools are subject to change at the discretion of the Government. The EA repository supports standard modeling notations as set forth in the Organizational Transformation Framework for Assessing and Improving EA Management, modeling tools (import/export from models), and the storage of artifacts and work products in a single place with version control and configuration management. It also provides executives, managers, staff, and authorized contractors a place to design, capture, view, and collaborate on the information that defines how AFRC operates within the one military operational EA net-centric arena.

2.9.2.1. **Contractor shall ensure the following tasks are accomplished:**
- Provide technical support, implementation, and management of the Government-specified AFR EA support tools, apps, data repository.
- Provide analysis, recommendation, and maintenance of EA tools which support EA design activities.
- Generate and/or maintain EA standards and processes (e.g., Standard Architecture templates used in architectural design); research and review existing EA standards and develop new EA policies and procedures, as needed.
- Provide artifact access to qualified AFR stakeholders and partners, and develop tools and methodologies to support service lifecycle management activities.
- Perform and maintain backup/recovery procedures and activities for all EA tools implemented.

- Perform administrative and configuration management related tasks for all EA tools implemented.
- Research and evaluate EA business process management tools, as required.
- Develop and maintain an AFRC EA Continuity of Operations (COOP) Plan. All processes and procedures documented in the COOP shall adhere to DOD and AFRC security policies and procedures, as well as industry best practices. COOP tasks shall include, but are not limited to:
  - EA Tool and server contingency plans (e.g., server or network issue contingencies, documentation of prior issues encountered and resolutions)
  - EA data back-up strategy and data configuration management plan
  - EA tool documentation and regularly scheduled administrative task SOPs
  - The COOP plan shall be posted in a common electronic area, as designated by the Government, for review and access (SharePoint or Shared Drive access), as well as a paper copy for offline reference. Furthermore, it shall be maintained throughout the life of the contract with quarterly updates due the 1st work day of each quarter thereafter. The COOP plan will be approved by the Government.
- Performs daily incremental and weekly full EA data backups.
- Troubleshoot issues impacting the EA technical environment to ensure technical environment remains operational.
- Assist the HQ AFRC ISSM with IA and C&A.

2.9.2.2. Qualifications:
- Significant experience as a MS SQL database administrator.
- Proficient in MS Office tools, including MS Project and Visio.

2.9.2.3. Certifications:
- 8570 certification required; IAT Level 2 certification is required.

2.9.2.4. Deliverables:
- AFRC EA Continuity of Operations (COOP) Plan delivered within 60 days of the beginning of period of performance (POP) with quarterly updates thereafter. **(CDRL A008)**

2.10. <u>IT Equipment Control (EC) Support – (SC)</u>. HQ AFRC utilizes the Asset Inventory Management System (AIMS), which is a database that manages and maintains physical accountability of all Air Force IT hardware assets. HQ AFRC ECOs currently manage 89 IT asset accounts and approximately 17,000 assets in AIMS.

2.10.1. Contractor shall ensure the following tasks are accomplished:
- Serve as the Alternate Equipment Control Officer (ECO) IAW AFMAN 33-153.
- Schedule classroom and provide training to Information Technology Equipment Custodians (ITECs) at Robins annually for primary and alternate ITECs for 89 accounts.

- Prepare quarterly ITEC training updates to keep ITECs current on procedures.
- Maintain listing of donation eligible customers to receive excess equipment.
- Maintain all accountability for excess equipment through inventory database.
- Prepare documentation for asset deliveries, secure storage, and transfer functions.
- Utilize the Asset Inventory Management System (AIMS) to add, edit, and delete IT asset records to provide management reports.
- Assist with IT inventories and Reports of Survey.
- Provide ITECs with current inventory listings and listing of assets requiring DRMO per annual tech refresh requirements.
- Direct ITECs to complete annual IT inventories and annual ITEC training, and distributes listing of noncompliant accounts and overdue training to leadership as necessary.
- Maintain up-to-date listings of ITEC appointments (including appointment letters) and ITEC annual training dates; distribute listings to ITEC directorate leadership for validation during annual inventory and tech refresh cycles.
- Sign off personnel out-processing checklist item for departing ITEC personnel, if new ITEC designation and loss-gain inventory completed by outgoing and incoming ITECs.
- Suspend processing of ITEC actions for inventory accounts, if annual account inventory or ITEC annual training is past due/non-compliant.
- Complete inventories upon arrival/acceptance, remove, pack and ship equipment components and once received, replace and/or connect these repaired components into their appropriate systems.

2.10.2. Qualifications:

- Significantexperience as an ECO.
- Packages may weigh as much as 50 pounds each as part of performing duties above.

2.10.3. Certifications:

- Required to achieve and maintain forklift certification required by host installation.

2.10.4. Deliverables:

- Status reports of task activities, as required. **(CDRL A009)**
- Trend and performance analysis reports. **(CDRL A010)**

2.11. Support Services, Package Delivery and Receipt of IT Equipment Support – (SC). HQ AFRC maintains customer service area in basement of Bldg 210 for parcel delivery, pick-up, outgoing shipments via commercial carriers, and the central collections area for recyclable printer toner cartridges. Approximately 160 outgoing parcels and 375 incoming parcels processed per month.

2.11.1. Contractor shall ensure the following tasks are accomplished:

- Provide services for receiving, processing, distributing, and dispatching official and accountable mail and administrative communications for HQ AFRC supported activities. These services must be IAW DoDM 4525.8, *Official Mail Manual*, DoDM 4525.6, Vol II, *Military Post Office Operation Procedures*, Domestic Mail Manual (DMM) and the International Mail Manual (IMM).
- Store received express mail/packages of IT equipment, using existing secure mail distribution room/boxes.
- Receive and distribute express mail/packages from private carriers.
- Provide postal/parcel services to include receipt, storage, distribution, and accountability of packages containing IT equipment.
- Assist customers in preparing express mail for pickup and to accept express mail deliveries of IT equipment.

2.11.2. Qualifications:

- Capable of lifting up to 50 pounds as part of performing duties above.

2.11.3. Certifications:

- Required to achieve and maintain forklift certification required by the host installation.

2.11.4. Deliverables:

- Status reports of task activities, as required. **(CDRL A009)**

2.12. <u>Command Electromagnetic Radio Frequency (RF) Spectrum Support – (A6OS)</u>. HQ AFRC/A6 is responsible for a wide variety of analytical planning and program management tasks related to electromagnetic RF spectrum support. On average, 180 permanent and 6 temporary frequency assignments requests are processed annually.

2.12.1. Contractor shall ensure the following tasks are accomplished:

- Perform staffing functions as designated technical and interface liaison between AFRC host bases and AFRC tenants (installation spectrum managers and spectrum users), FAA, FCC, Air Force Spectrum Management Office (AFSMO) and HQ AFRC;
- Act as the spectrum Subject Matter Expert to provide a range of support from processing permanent and temporary assignments, and resolving spectrum interference issues within United States and with US bordering countries.
- Implement rules, regulations and policies as established by the National Telecommunications and Information Administration (NTIA), International Telecommunication Union (ITU), Military Communications Electronic Board (MCEB), Joint Spectrum Center and Military Departments to support AFRC operations world-wide.
- Provide recommendations on issues relating to and impacting availability of the radio frequency spectrum.

- Engineer, nominate, coordinate, and recommend assigned frequencies to support AFRC communications, operations and exercise requirements. Ensure frequency allocations and assignments are properly coordinated and processed in a timely manner for electromagnetic radiating devices essential for the operations for radio circuits, RADAR, microwave systems, equipment under range instrumentation facilities, telemetering, navigational aids, Land Mobile Radio (LMR) as required by all AFRC radio spectrum users.
- Prepares and submits DD Form 1494, **Application for Equipment Frequency Allocation**, and monitors through completion.
- Analyze and de-conflict radio frequency requirements for compatibility with other users of the Electromagnetic spectrum and coordinates frequency needs with federal [Federal Aviation Administration (FAA)], military (DoD Area Frequency Coordinator), and civil spectrum agencies [Federal Communications Commission (FCC)] to resolve radio frequency interference and protect national spectrum resources.
- Evaluate new or significantly modified RF equipment detailed in spectrum certification and submits application for frequency allocation and Standard Frequency Action Format (SFAF) in a timely manner throughout the command, and monitor requirements for timely responses from national-level agencies involved in spectrum management.
- Ensure frequency assignment records in the Government Master File (GMF) and Frequency Resource Record System (FRRS) are up-to-date and maintained in accordance with (IAW) governing directives.
- Keep customers informed of current status on frequency proposals and provides notification of assignment parameters and limitations.
- Assist organizations from degrading friendly systems or operations during command, control, and communications countermeasures training activities.

2.12.2. Qualifications:

- Extensive experience in the area of DoD Spectrum Management.
- Proficient with Joint Data Access Web Server (JDAWS) Spectrum Certification Software (SCS) or the Equipment Location-Certification Information Database (EL-CID) Analysis tools.
- Knowledge of radio, radar, concepts, principles and practices related to the management of the electromagnetic spectrum.

2.12.3. Certifications.

- Graduate of the Inter-service RF Spectrum Management School.
- Graduate of the Joint Spectrum Center's Spectrum XXI Course.

2.12.4. Deliverables:

- Metrics on overdue assignments, significantly overdue assignments, and interference issues, quarterly. **(CDRL A012)**

2.13. <u>Cyber Force Development Support – (A6OD)</u>. HQ AFRC/A6 is responsible for force readiness analysis to include force management metrics, processes, and procedures. Key areas include cyber education, manning, and other force development core competencies.

2.13.1. Contractor shall ensure the following tasks are accomplished:

- Provide support for career development, force readiness, and training.
- Develop, define, and document new or evolving metrics and demographics for functional managers, career field managers, and other customers.
- Provide research, compilation, and data analysis on metrics and demographics for all functional managers.
- Provide research, compilation, and data analysis on manpower authorizations and/or assigned personnel for MAJCOM Career Field and Functional Managers (MFMs) for purposes of metrics and tracking changes in end strength.
- Review, research, coordinate, and utilize Unit Manning Documents (UMDs), Unit Manpower Personnel Roster (UMPRs), Unit Training Assembly Participation System (UTAPS), Air Force Reserve Orders Writing System-Reserve (AROWS-R), Military Personnel Data Systems (MILPDS), and other documents to create accurate career field documents and briefings (e.g., Cyber Health Briefs for all assigned cyber AFSCs; currently 17XXX, 3DXXX, 1B4XX, 3A1XX; Staff-to-Staff submittals, all status allocations by MAJCOM/Combatant Commander (COCOM)/Agency).
- Provide SharePoint site administration and Training Business Area (TBA) to functional managers, career field managers, and other customers.
- Develop and assist functional managers, career field managers, and other customers in creating routine functional newsletters to the field.
- Draft SOPs for tasks accomplished within the branch or division.
- Receive allocations, registers, tracks, and monitors attendance for various cyber training courses.
- Provide support for pre/post-Development Team (DT) tasks.
- Perform division submissions of new metrics entering the Internal Control Measure (ICM) tool process. Provide quality control and updates to existing metrics in ICM. Ensure adherence of standards on submittals to ICM Business Rules.
- Review, track, collate, and provide accurate position data across all statuses (AD, AGR, ART, IMA, and TR); specifically, vacancy/fill rates, pending change actions such as reorganizations, IMA Internal Program Reviews (IPRs), Program Objective Memorandum unit activations/deactivations, and other programmatic changes.
- Dissemination of routine position vacancy announcements to the field.
- Engage MAJCOM Functional Managers (MFMs) on records management status, develop and follow standard business rules (such as location, access, and classification of records).

2.13.2. Qualifications:

- Knowledge of the following programs:
  - Microsoft Excel (pivot tables, data sorting, filtering, etc.).
  - MS PowerPoint (creating and updating presentations).
  - MS SharePoint (administration, create pages, update pages).

2.13.3. Certifications:

- None required.

2.13.4. Deliverables:

- Draft and final standard operating procedures and business rules for the functional managers, as required, are accomplished. **(CDRL A013)**
- Position Descriptions both military and civilian. **(CDRL A013)**
- Current and projected position data across the cyber position enterprise. **(CDRL A014)**
- Status reports of task activities, monthly. **(CDRL A009)**
- New technology research briefings/reports, as required. **(CDRL A011)**
- Trend and performance analysis reports, as required. **(CDRL A010)**

3. ENTERPRISE/NETWORK SERVICES AND COMMUNICATIONS SUPPORT AT HQ AFRC AND AFRC HOST BASES. HQ AFRC is responsible for the operation, management, administration, and user support for the information technology environment at HQ AFRC, and other sites referenced in Table 3. AFRC is forward-thinking and continually inserts new technology into our operational environment. Additionally, there are a number of initiatives that AFRC will participate in such as consolidating data centers, integrating into the Joint Information Enterprise (JIE), cloud environments, mobile framework and Defense Information Systems Agency (DISA) environments. Workload will include Service Oriented Architecture (SOA) tools, business analytics, and dashboard implementation.

Support is required to maintain, enhance, and improve the sites in an operational status by supporting all fielded (and planned) network support systems, and projects/tasks required by the Government on NIPR and SIPR. The Government base support may include other tenants.

The AFRC NIPR/SIPR network environment consists of approximately 12 Local Area Networks (LANs), 1,253 servers, 20,314 workstations and 2,000 cellular mobile devices at multiple buildings and sites. AFRC utilizes desktops, laptops, and zero clients on NIPR and SIPR.

Systems are Government owned-server based systems using approved Windows Workstation Operating Systems and approved Microsoft server Operating Systems. The configuration will change during the course of the contract as sites move toward standardized Commercial Off-the Shelf (COTS) software and hardware to complete the

open system architecture. Migration to Windows 10 (SDC-5.x) will continue and potentially new OSs will occur. AFRC is currently Windows Server 2012 but will move shortly to Windows Server 2016. Vendors should plan accordingly.

AFRC uses the following list of standard equipment and COTS software. Non-standard software and hardware will be secondary. Additional brands of equipment and software could be procured separately during this contract period and will also be covered.

3.1. Hardware:

Network Servers	SAN/NAS Storage Systems
Routers	Windows Desktop, Laptop, and Zero Clients PCs
Wireless Access Points	UPS
Network Switches	HP-UX
Dell	Egan Marino Corporation (EMC)
Cisco	

3.2. Software:

MS Office Suite (2010, 13, 16)	Remedy Management System (RMS)
Microsoft Exchange (future in the cloud with Collaboration Pathfinder)	Microsoft BackOffice
SQL 2012 and newer	HP Net Management
Pure Edge	Windows Active Directory
SharePoint	TMG/F5
Management Information Base (MIBS)/Server Message Block (SMB)	Virtustream
Network File System (NFS) and SMB	Third Party software as required
Lync/DCS	PowerShell
Cisco Prime Infrastructure VMWare vRealize	Customer Relationship Management (CRM)
	System Center Operations Manager (SCOM)
Network Browsers (Microsoft Edge, FireFox/Mozilla, Chrome, IE)	Microsoft System Center Configuration Manager (MS SCCM)

3.3. Operating Systems:

CISCO IOS	Windows operating systems including:
F5	Windows Win 8 and Win 10
Cisco CAT OS	Windows Server 2008, 2012, and 2016

Note: The above lists common hardware, software and operating systems currently in use by AFRC. Other hardware, software, and/or operating systems may be utilized.

3.4. AFRC Services Support. AFRC performs a number of tasks described below for the AFRC user community and AFRC host bases. The tasks below are executed from HQ AFRC and/or at locations specified (Table 3). AFRC supports 25,000 users at AFRC host bases and an additional 47,000 users at AFRC tenant locations. Additional scoping information is included in each applicable services requirement.

3.4.1. Each function below (3.4.1. thru 3.4.14; 3.4.17., and 3.7.3.) shall provide/execute the following set of common tasks, in addition to the tasks listed under each function:

- Coordinate with HQ/base CFPs or CSC for issue resolution.
- Coordinate with ESU, INOSC-E, MAJCOM Communications Coordination Center (MCCC), CFP, AFRC host bases, etc.… on day-to-day support/maintenance activities on the servers and services.
- Contact the appropriate Government and/or commercial agencies to resolve maintenance problems.
- Ensure backups and monitoring are being accomplished in accordance with applicable procedures.
- Coordinate, document, test, validate, and deploy new technology provided by government.
- Provide physical server support.
- Utilize Remedy to document, coordinate, route, resolve, and close user issues and server/services issues.
- Conduct/assist with installs/configurations of the hardware and software for appropriate servers to Air Force specifications.
- Conduct defensive missions to operationally protect the enterprise.
- Determine and mitigate AFNet/JIE caused issues to AFRC missions.
- React to and remediate AFNet service interruptions.
- Support/complete Certification and Accreditation (C&A) activities for 3.4.2. thru 3.4.14; 3.4.17., and 3.7.3.
- Participate in Government program/project reviews, technical meetings, and briefings.
- Remediate vulnerabilities on assigned hardware and software.
- Work, coordinate, document, resolve, and close trouble tickets assigned to and within the work center.
- Ensure compliance with DISA STIGs, AF instructions and orders on assigned systems.
- Implement change requests approved by AFNet configuration management processes for assigned function.
- Assist AFRC host bases in virtual management issues, installs, projects, etc.
- Ensure NIPR/SIPR CAT vulnerabilities for each assigned server does not exceed AFRC, AF, DISA, or DoD vulnerability thresholds; must be $\leq$2.49 vulnerabilities per each assigned server.
- Server administrators will implement AF Maintenance Tasking Orders (MTOs), TCNOs, and CCOs by established deadlines and with minimum 95% compliance

for MTOs; 100% compliance for TCNOs and CCOs. All non-compliant MTOs will be corrected within 5 days.

- Meet individual project schedule milestones for key projects designated by the Government; meet project schedule milestones on-time delivery at or above 90% level. Late deliveries must not be more than 5 days late.

3.4.2. Engineering and Infrastructure Project Oversight Support - (SC):

3.4.2.1. Contractor shall ensure the following tasks are accomplished:

- Monitor the task activities for the Government for supported Enterprise functions.
- Task activities include, but are not limited to, projects, upgrades, remediation actions, and new technology insertion.
- Provide overall oversight of the functional areas work plans.
- Manage and maintain VMs and virtualization related technologies, including Configuration Management tools.
- Identify trade-offs between short and long term goals with the needs of stakeholders. Develop positive cross-functional relationships between business units, human resources, IT, and other groups to track service levels.
- Align tasks with business' goals and understand connections across organizational boundaries.
- Ensure cross-functional projects are aligned with the overall goals.
- Provide information and input into to the local configuration control process.
- Document service offerings.
- Assist in adherence to audit, legal and compliance governance issues relative to services offered.
- Maintain technical knowledge in services offered and operational management of those services; review professional publications; assist to benchmark state-of-the-art practices.
- Provide input for training, process or equipment deficiencies.
- Facilitate lateral and vertical communication related to the tasks/activities.
- Coordinate at all levels--with technicians and AFRC leadership, AFNet operational organizations and staff organizations such as an Air Force Space Command (AFSPC), Air Force Network Integration Center (AFNIC), 24th Air Force (24 AF).
- Coordinate within AFRC and other MAJCOMs for AFNet support and coordinating team support to those organizations.
- Coordinate with appropriate Enterprise Service Unit (ESU), Integrated Network Operations Security Center (INOSC) or other external agencies, as required, to ensure AFNet issues are being resolved.
- Coordinate with agencies to ensure new, deployed technologies are documented, tested, and validated.
- Conduct new technology research.
- Establish a program to document, trend, and perform analyses on performance and assigned task accomplishment.

3.4.2.2. Qualifications:

- Significant experience with AFNet projects.
- Experience in AFNet Enterprise Services delivery.

3.4.2.3. Certifications:

- 8570 certification required; IAT Level 2 certification is required.

3.4.2.4. Deliverables:

- Status reports of task activities, as required. **(CDRL A009)**
- New technology research briefings/reports, as required. **(CDRL A011)**
- Trend and performance analysis reports. **(CDRL A010)**

3.4.3. <u>Virtualization Engineering and Management Support - (SC)</u>. AFRC manages 18 data centers for 12 locations that incorporate 21 VMware suites, 501 virtual servers, and approximately 300 virtual desktops. The virtual desktops will continue to increase during the contact period. AFRC also centrally manages the AFRC NIPR/SIPR environment for a user population of approximately 25,000 regular users and up to 70,000 users during peak times.

3.4.3.1. Contractor shall ensure the following tasks are accomplished:

- Manage multiple virtual server platforms.
- Manage and secure Virtual Desktop Infrastructures [Virtual Local Area Network (VDIs)] (zero clients) and the environment.
- Manage the variety of application deployment methods including application virtualization, thin applications, Application Volume, and Security Server.
- Support externally facing customers with Security Server for virtual desktops.
- Serve as focal point for AFNet issues and user problem resolution in the virtual suites.
- Provide operational support for applications, systems, or infrastructure.
- Conceptualize, architect, design, implement and support integrated solutions in support of business demand.
- Work with enterprise architects to ensure the cloud infrastructure architecture is aligned with enterprise architectural standards and strategies.
- Apply architectural standards within the cloud infrastructure operation including operational considerations in cloud infrastructure architecture and design.
- Support efforts to architect and design cloud infrastructure extensions.
- Architect and design the cloud layer in support of the planned cloud-based services as well as any changes.
- Identify market needs for new products or technologies and/or how current products can be modified or enhanced. Identify ways in which new products and/or modifications or enhancements to current products can be successfully implemented.
- Deploy large scale cloud infrastructure and application services for customers.

- Implement and configure virtualized infrastructure.
- Participate in design and implementation activities with emphasis on supportability, maintainability, scalability, performance and overall quality.
- Utilize virtualization tools to deliver user-facing capabilities, track utilization and automate delivery of services.
- Offer overall support for virtualized infrastructure environment.
- Provide support across the entire platform stack for innovative cloud-based solutions from the virtualization layer up through the software-defined and cloud management platform stacks.
- Establish and/or manage on-prem and hybrid cloud technologies (e.g., EMC's VMware & Virtustream)
- Apply DoD/AF Cloud strategies to include standards and operational considerations in cloud infrastructure architecture and design
- Identify issues/problems with Cloud implementation and recommend specific solutions

3.4.3.2. Qualifications:

- Technical experience working in a VMware environment.
- Technical experience utilizing vRealize.
- Technical experience utilizing PowerShell.
- Knowledge of infrastructure (including VLANs) and storage environments, and basic networking knowledge.
- Experience with Microsoft Windows Server 2008R2 or newer.

3.4.3.3. Certifications:

- 8570 certification required; IAT Level 3 certification is required.

3.4.3.4. Deliverables:

- Status reports of task activities, as required. **(CDRL A009)**
- New technology research briefings/reports, as required. **(CDRL A011)**

3.4.4. Database Administration Support - (SC):

3.4.4.1. Contractor shall ensure the following tasks are accomplished:

- Plan, design, enforce and audit security controls, policies and procedures which safeguard the integrity of and access to data.
- Ensure security controls meet all legal, contractual, regulatory and business requirements and contractual agreements.
- Ensure data is accessible and recoverable.
- Install and maintain databases for COTS products and designs and implements custom application databases to support a highly secure environment.
- Support the development, test and production environments.
- Identify performance improvement areas for databases.

- Write procedural documents (How-To) to document the installation of products and maintenance procedures.
- Support engineers and developers in troubleshooting issues with their products and custom code.
- Work with project personnel to resolve schedule problems and ensure developed applications and systems are transitioned to production in a timely manner.
- Identify and manage dependencies with other systems and elements of the IT infrastructure.
- Provide tools and documents to AFRC tiered support work centers to aid in customer support, trouble shooting and determining the severity of issues.
- Provide AFRC tiered support work centers with information for customer training.

3.4.4.2. Qualifications:

- Technical experience working in a database environment.
- Technical experience utilizing PowerShell.
- Experience with Microsoft Windows Server 2008R2 or newer.
- Experience with database administration with emphasis in MySQL, MS SQL Server and PostgreSQL and/or Oracle 11g.

3.4.4.3. Certifications:

- 8570 certification required; IAT Level 2 certification is required.

3.4.4.4. Deliverables:

- Status reports of task activities, as required. **(CDRL A009)**
- New technology research briefings/reports, as required. **(CDRL A011)**

3.4.5. <u>Directory Services (DS) Support - (SC)</u>. AFRCs environment supports activities for 25,000 regular users and up to 70,000 users at peak times on NIPR and 3,000 users on SIPR. There are approximately 60 Domain Controllers for authentication services and policy enforcement for approximately 25,000 workstations on NIPR and 10 Domain Controllers and 600 workstations on SIPR. There are approximately 10 authentications and load balancing servers [currently Threat Management Gateway (TMG) for approximately 10,000 simultaneous users].

3.4.5.1. Contractor shall ensure the following tasks are accomplished:

- Participate in design and implementation activities with an emphasis on supportability, maintainability, scalability, performance and overall quality.
- Provide support for innovative cloud-based solutions from the virtualization layer up through the software-defined and cloud management platform stacks.
- Support for other roles involved in the cloud environments.
- Plan, design, enforce and audit security controls, policies and procedures which safeguard the integrity of and access to data.

- Identify improvements for processes and procedures, and introduce automation to improve.
- Establish, administer, and manage domain controllers.
- Establish, administer, and manage the Key Management Server (KMS), Dynamic Host Configuration Protocol (DHCP), command Login Script, Distributed File System (DFS), and File Transfer Protocol (FTP) server.
- Establish, administer, and manage authentication and load balancing servers.
- Authenticate and load balance servers (currently Threat Management Gateway (TMG).

3.4.5.2. Qualifications:
- Technical experience working with Directory Services.
- Technical experience utilizing PowerShell.

3.4.5.3. Certifications:
- 8570 certification required; IAT Level 2 certification is required.

3.4.5.4. Deliverables:
- Status reports of task activities, as required. **(CDRL A009)**
- New technology research briefings/reports, as required. **(CDRL A011)**

3.4.6. <u>Cyber Transport (CT) Support – (SC)</u>. AFRC has approximately 1700 infrastructure devices (NIPR/SIPR) across the HQ AFRC and AFRC host bases. Each base has approximately 125 devices (on average) per base—except ARPC has approximately 10 (NIPR only). The remaining devices are at HQ AFRC. These devices include, but are not limited to, TACLANES, switches, routers, Call Manager, and authentication servers. Also included are VoIP/VoSIP devices (one per person) at AFRC host bases (approximately 25,000). It also has approximately 8 authentication and load balancing servers (currently F5) that services approximately 10,000 simultaneous users.

3.4.6.1. <u>Enterprise CT Support – (SC)</u>:

3.4.6.1.1. Contractor shall ensure the following tasks are accomplished:
- Provide Enterprise (NIPR/SIPR) MAN/LAN/WAN administration, network configuration, infrastructure management for servers, switches, routers, wireless infrastructure, cellular, and UPS/power systems.
- Support domain name service (DNS) for Enterprise.
- Design, plan, manage, maintain, and support network-related infrastructure.
- Support cloud efforts with network design and technical direction.
- Ensure the technical environment is properly maintained and correctly designed.
- Support development and integration of cloud application and infrastructure services into existing systems.
- Assist with ongoing build out of the cloud platform.

- Assist the coordination of testing efforts and identify and resolve system integration issues.
- Maintain and improve IT infrastructure and cloud environment.
- Identify improvements for processes and procedures, and introduce automation to improve.
- Configure and maintain system, network, service, and user accounts for Enterprise CT functions.
- Establish, configure, administer, and manage authentication and load balancing servers.
- Monitor security of devices and implement new configurations and/or IOS upgrades for Enterprise devices.
- Monitor and reports Enterprise WAN bandwidth utilization and circuit latency.
- Manage Enterprise CT software configuration management.
- Ensure Enterprise complies with AF Base Area Network (BAN) functional specification.
- Plan and execute Enterprise software and hardware upgrades and revisions.
- Conduct system analyses to resolve configuration and equipment problems.
- Provide recommendations and return sites to an operational status.
- Troubleshoot Enterprise hardware, software and network problems.
- Serve as focal point for problem resolution for Enterprise CT issues.
- Support migration from legacy to VoIP.
- Implement, maintain, and upgrade UCS hardware/software.

3.4.6.1.2. Qualifications:

- Technical experience in AFRC and AFNet.
- Technical experience utilizing Cisco devices.
- Technical experience utilizing Cisco Call Manager.

3.4.6.1.3. Certifications:

- 8570 certification required; IAT Level 2 certification is required.

3.4.6.1.4. Deliverables:

- WAN bandwidth utilization and latency reports, monthly. **(CDRL A015)**

3.4.6.2. HQ AFRC and AFRC Host Base CT Support:

3.4.6.2.1. Contractor shall ensure the following tasks are accomplished:

- Provide the following functions for the respective location (see Table 3):
  - Provide NIPR/SIPR LAN administration, network configuration, and infrastructure management for servers, switches, routers, wireless infrastructure, cellular, and UPS/power systems.
  - Provide physical support in wiring/re-wiring comm closets, cubicles, office, etc., supporting user moves, building renovations, etc.
  - Manage Internet Protocol address space.

- Support domain name service (DNS).
- Configure and maintain system, network, service, and user accounts for CT functions.
- Monitor security of devices and implement new configurations and/or IOS upgrades.
- Establish, configure and maintain Cisco Access Control Server (ACS).
- Monitor and report LAN bandwidth utilization and circuit latency.
- Manage CT software configuration management.
- Ensure compliance with AF Base Area Network (BAN) Functional Specification.
- Install and sustain VoIP devices, switches, and cable.
- Plan and execute software and hardware upgrades and revisions.
- Conducts system analyses to resolve configuration and equipment problems.
- Provide recommendations and return sites to and buildings and nodes to operational status.
- Troubleshoot hardware, software and network problems.
- Manage local DHCP.
- Build and maintain Virtual LANs (VLANs)
- Manage local Call Manager.
- Manage local UCS and ACS.
- Manage local TACLANES.
- Manage local wireless and cellular capabilities.
- Serve as the local focal point for problem resolution for CT issues
- Mature migration from legacy to VoIP.
- Ensure physical security/maintenance of CT hardware NIPR/SIPR

- ARPC specific:
  - Provide Cisco Unified Call Center Express (UCCX) suite capabilities including Agent Desktop maintenance which also includes computer telephony integration (CTI) support.
  - Provide Interactive Voice Response (IVR) capability and sustainment using the CISCO or other platforms to include Genesys and Quality Management System.
  - Work with the local base telephony authority to resolve and repair communications circuit and digital gateway issues that enter and transverse the ARPC facility.

3.4.6.2.2. Qualifications:

- Technical experience in AFRC and AFNet.
- Technical experience utilizing Cisco devices.
- Technical experience utilizing Cisco Call Manager.
- Knowledge of IVR scripting using voice extensible markup language or other common IVR programming languages.

3.4.6.2.3. Certifications:

- 8570 certification required; IAT Level 2 certification is required.

3.4.6.2.4. Deliverables:

- WAN bandwidth utilization and latency reports, monthly. **(CDRL A015)**
- Status reports of task activities, as required. **(CDRL A009)**
- New technology research briefings/reports, as required. **(CDRL A011)**

3.4.7. Messaging Support – (SC). AFRC supports daily messaging activities for 25,000 users with an additional, potential user base of up to 47,000 more users on NIPR. AFRC expects to transition to another email provider in FY17-18. However, it is expected that the Mobile Device Management (MDM) capability (currently Blackberry) for the mobile devices will remain at AFRC during this contract period. There are approximately 10 Microsoft Exchange servers, 3 Client Access Servers (CAS), 3 Hub Transport (HT) servers, Blackberry/Dynamics servers, Outlook Web Access (OWA), Outlook Anywhere, and other miscellaneous servers/services supporting messaging in the AFNet.

3.4.7.1. Contractor shall ensure the following tasks are accomplished:

- Support daily messaging activities.
- Serve as focal point for messaging problem resolutions user issues (on-premises and/or Collaboration Pathfinder) (Tier 2), system issues, security updates, server maintenance, and AFNet issues.
- Install, configure, operate, and maintain network messaging applications.
- Maintain accuracy of the Global Address List (GAL) as well as local Address Lists.
- Troubleshoot wide area mail flow.
- Make recommendations for the command's effort for AFRC messaging policies, management, and new mobile technologies.
- Support Android, Apple, Windows, Blackberry/Good, and other devices/capabilities AFRC pursues.
- Track Blackberry/Good user license usage and eliminate unused license usage by coordinating with HQ and base CFPs.

3.4.7.2. Qualifications:

- Technical experience in AFNet.
- Technical Experience in performing Microsoft (MS) Exchange E-mail system administration.
- Technical experience with PowerShell.

3.4.7.3. Certifications:

- 8570 certification required; IAT Level 3 certification is required.

3.4.7.4. Deliverables:

- Blackberry/Good usage statistics, as required. **(CDRL A016)**
- Blackberry/Good license usage, as required. **(CDRL A016)**
- Status reports of task activities, as required. **(CDRL A009)**

- New technology research briefings/reports, as required. **(CDRL A011)**

3.4.8. <u>Mobile Application Infrastructure Support – (SC)</u>. HQ AFRC supports an ,initial mobile application with 7,000 users. It is expected that during this contract period, the number of mobile applications will increase from 1 to approximately 40. AFRC's user base for the mobile applications is 70,000 users. The current MDM is Blackberry Dynamics/Blackberry Work but VMware's Airwatch and other MDMs will be evaluated and potentially used for mobile application deployment and management.

3.4.8.1. Contractor shall ensure the following tasks are accomplished:

- Deploy, create, configure, and administer cloud provider-related components and cloud-specific operational management tools.
- Support efforts to configure and implement any required cloud integration with other applications, automation monitoring and automated event/ incident remediation wherever possible and appropriate.
- Support innovative cloud-based solutions from the virtualization layer up through the software-defined and cloud management platform stacks.
- Configure, manage, secure, patch, and maintain the mobile application infrastructure servers and capabilities.
- Serve as focal point for mobile user problem resolutions (Tier 2), system issues, security updates, server maintenance, and AFNet issues.
- Make recommendations for the command's effort for AFRC mobile policies, management, and new mobile technologies.
- Support Android, Apple, Windows, Blackberry and other devices/capabilities AFRC pursues.
- Track user license usage and eliminates unused license usage by coordinating with HQ and base CFPs.
- Minimizes services, application, and system unscheduled downtime with 99% availability for the month with no more than 7 hours of downtime within contractor's control.
- Design/implementation/management of Mobile infrastructure (e.g., BlackBerry Work, BlackBerry Dynamics, Airwatch)
- Identification of issues/problems with Mobile implementations and recommended specific solutions
- Enterprise Mobility Management for Apple iOS, Android, and Window devices to include Mobile Device Management (MDM) and Mobile App Management (MAM) Mobile Content Management (MCM)

3.4.8.2. Qualifications:

- Technical experience in AFNet.
- Technical experience with Mobile Device Management (MDM) solutions.
- Technical experience with Mobile Application Management (MAM) solutions
- Technical experience with PowerShell.

3.4.8.3. Certifications:

- 8570 certification required; IAT Level 3 certification is required.

3.4.8.4. Deliverables:

- MDM and MAM usage statistics, as required. **(CDRL A017)**
- Trend and performance analysis reports (e.g., license usage), as required. **(CDRL A010)**
- New technology research briefings/reports, as required. **(CDRL A011)**
- Status reports of task activities, as required. **(CDRL A009)**

3.4.9. Enterprise File/Storage Support – (SC). HQ AFRC **s**upports NIPR/SIPR daily file storage, backup, and restoration process for AFRC. Current user population is approximately 25,000 users and approximately 850 servers/appliances/devices.

3.4.9.1. Contractor shall ensure the following tasks are accomplished:

- Serve as focal point for problem resolution and is the primary point of contact for problems relating to AFNet issues and AFNet user issues on file storage, backup, restoration, etc.
- Work with users and organizations to standardize file storage directory structures.
- Ensure data is accessible and recoverable.
- Identify improvements for processes and procedures, and introduce automation to improve.
- Participate in design and implementation activities with an emphasis on support, maintenance, scale, performance and overall quality.
- Support innovative cloud-based solutions from the virtualization layer up through the software-defined and cloud management platform stacks.
- Actively monitor, update, and correct file/storage access permissions.
- Monitor and conduct file/storage backups and restores.
- Coordinate to monitor and execute core and non-core servers and services restores (including user email restores).

3.4.9.2. Qualifications:

- Technical experience in AFNet.
- Technical knowledge of VMware, Directory Services (DS), and CT.
- Technical experience with Virtual CIF File Servers, Storage Area Network (SAN), and Network Attached Storage (NAS).
- Technical experience with PowerShell.

3.4.9.3. Certifications:

- 8570 certification required; IAT Level 3 certification is required.

3.4.9.4. Deliverables:

- Trend and performance analysis reports (e.g., file storage usage metrics), as required. **(CDRL A010)**

- New technology research briefings/reports, as required. **(CDRL A011)**
- Status reports of task activities, as required. **(CDRL A009)**

3.4.10. AFRC Wide Area/I-COOP File Server Storage Support – (SC): HQ AFRC **s**upports an enterprise Information Continuity of Operations Capability (I-COOP).

3.4.10.1. Contractor shall accomplish the following tasks:

- Serve as focal point for problem resolution on EMC Storage File Server Consolidation devices and Information Continuity of Operations Capability (I-COOP) backup monitoring and replication issues.
- Perform system analyses to resolve configuration and equipment problems.
- Coordinate with HQ and base CFPs to schedule hardware and software maintenance and updates to the storage equipment.
- Schedule and execute backups, test, and monitor successful backup replication and recovery operations to ensure successful and optimum performance of data recovery and backup capability.
- Provide Tier 2/3 support to HQ/bases CFPs on storage, backup, restores, and remediate user-based, system-based, AFNet-based, etc. issues.
- Support all aspects of the I-COOP File Server Consolidation to include; shares creation on the devices, privileges to file share areas, allocation of file share space on base devices.
- Monitor storage devices for backup success, recovery success, capacity planning, and recommends expansion of devices as need arises.
- Build servers to support storage monitoring tools.
- Assist in new installs and configuration of file storage equipment.
- Monitor the day-to-day back-up operations of Avamar software for AFRC.
- Provides administration and configuration support for Avamar software operations.

3.4.10.2. Qualifications:

- Technical experience working and coordinating with AFNet.
- Technical knowledge of VMware, DS, and CT.
- Technical experience with File Servers, SAN, and NAS.
- Technical experience with PowerShell.
- Technical experience with EMC hardware/software and Cisco.
- Knowledge of hardware and software:
  - EMC Avamar Backup Software
  - EMC Avamar Data Migrator
  - EMC Avamar Data Replication
  - EMC DataDomain Backup (BU) Storage
  - EMC DataDomain BU Replication
  - EMC RECOVERPOINT (RPA)
  - EMC ViPR MANAGER
  - EMC VNX/VNX2

- EMC VPLEX
- EMC XTREM-IO (FLASH)
- EMC CIF Virtual Microsoft File Server configuration according to AF standards
- CISCO Fabric Manager
- CISCO Fabric Interconnect
- CISCO Fabric Switch

3.4.10.3. Certifications:

- 8570 certification required; IAT Level 3 certification is required.

3.4.10.4. Deliverables:

- New technology research briefings/reports, as required. **(CDRL A011)**
- Status reports of task activities, as required. **(CDRL A009)**

3.4.11. <u>Network Infrastructure Engineering Support – (SC)</u>. HQ AFRC provides AFRC-wide engineering of the overall architecture for HQ AFRC and AFRC host bases on NIPR and SIPR. This includes the WAN architecture supporting AFRC data centers, backbones, cloud initiatives, and mission data traversing the WAN. Infrastructure support includes oversight of the AFRC Enterprise comprising approximately 1,700 infrastructure devices on NIPR and SIPR.

3.4.11.1. Contractor shall ensure the following tasks are accomplished:

- Support high Temporary Duty (TDY) requirement (estimated to be 75%) due to high-level of base project support.
- Serve as focal point for AFRC IP space management.
- Serve as focal point for the infrastructure engineering for AFRC.
- Manage technology refresh for the command.
- Make recommendations to the Government for infrastructure upgrades, configurations, efforts at HQ and bases. These include: Core Nodes (CN), Critical Distribution Nodes (CDN), Critical Access Nodes (CAN), Distribution Nodes (DN), and Access Nodes (AN).
- Coordinate, as technical liaison, technical requirements with the Government lead.
- Ensure enterprise network (NIPR/SIPR) compliance with AFR BAN functional specification.
- Function as SME for NIPR/SIPR) network-related IT requirement reviews.
- Function as SME for network Command Cyber Readiness Inspection (CCRI) support.
- Perform on-site Local and Wide Area Network (LAN/WAN) security management functions.
- Function as the SME for Air Force network projects effecting both the HQ and enterprise [e.g., Base Information Transport Infrastructure (BITI), One Base One Network (1B1N), Data Center Optimization Initiative (DCOI), Enclave NIPR

Firewall and ASIM Sustainment (ENFAAS), Installation Processing Node (IPN), etc.].
- Coordinate with AF project offices and AF responsible offices for Enterprise projects and programs impacting AFR equities.
- Assist with on-site system administration functions.

3.4.11.2. Qualifications:
- Extensive technical experience in AFRC architecture.
- Extensive experience designing, deploying, managing and supporting mission critical network environments based on Cisco hardware and Internal Operating System (IOS).
- Extensive experience with Air Force NIPR, SIPR and Combat Information Transport System (CITS) architecture and programs.
- Extensive experience as a project manager in data center migrations, enterprise network upgrades and WAN upgrades.
- Extensive experience in Local Area network design, configuration, installation, evaluation, problem resolution and project management.
- Knowledge of all common routing protocols, include, but are not limited to, Enhanced Interior Gateway Routing Protocol (EIGRP), Open Shortest Path First (OSPF), and Border Gateway Protocol (BGP).
- Knowledge of industry-standard network design principles and best practices.

3.4.11.3. Certifications:
- 8570 certification required; IAT Level 3 certification is required.
- Cisco Certified Associate Level (e.g., CCNA) or Cisco Certified Professional Level (e.g., CCNP) certification required.
-

3.4.11.4. Deliverables:
- New technology research briefings/reports, as required. **(CDRL A011)**
- Status reports of task activities, as required. **(CDRL A009)**

3.4.12. <u>Server/Infrastructure Monitoring Support – (SC)</u>. HQ AFRC provides monitoring support for the core and functional system owners and administrators. Monitoring of mission essential systems and infrastructure provides Situational Awareness (SA) for the Enterprise. Currently, this effort is supported with Microsoft System Center Operations Manager (SCOM) for approximately 210 servers, 14 systems, and 65 infrastructure devices across 12 AFRC locations on NIPR. AFRC is currently expanding monitoring on SIPR to mimic NIPR that will include approximately 45 servers, 6 systems, and 40 infrastructure devices. AFRC currently provides this capability for HQ AFRC servers/services but plans to expand to all of AFRC.

3.4.12.1. Contractor shall ensure the following tasks are accomplished:

- Perform persistent daily monitoring activities to the MAJCOM leadership, MCCC, functional system owners, core server/system owners and the entities requiring visibility of the current stability and availability of the Enterprise.
- Manage monitoring capability for all core and non-core systems/servers.
- Serve as focal point for problem resolution and is the primary point of contact for problems relating to AFNet issues and AFNet user issues relating to monitoring of servers, infrastructure, services, etc.
- Coordinate with servers/services owners on monitoring devices, servers and services and the respective thresholds.
- Ensure server/service owners and the operational teams receive their respective alerts accurately; modify as required.
- Minimizes services, application, and system unscheduled downtime with 99% availability for the month with no more than 7 hours of downtime within contractor's control.

3.4.12.2. Qualifications:
- Technical experience utilizing an AFNet-utilized monitoring tool (e.g., SCOM, and Solar Winds).
- Technical experience utilizing PowerShell.
- Technical experience with Microsoft Windows Server 2008R2 or newer.

3.4.12.3. Certifications:
- 8570 certification required; IAT Level 2 certification is required.

3.4.12.4. Deliverables:
- Trends and performance analysis reports (e.g., data of systems, servers and devices monitored and those not monitored), as required. **(CDRL A010)**
- New technology research briefings/reports, as required. **(CDRL A011)**
- Status reports of task activities, as required. **(CDRL A009)**

3.4.13. <u>SIPRNet/Global Command and Control System (GCCS) Support – (SC)</u>. Environment consists of approximately 3,000 users, 700 workstations, and 75 servers supporting virtual server environment hosting application and core servers/services and a virtual environment for command-wide virtual workstations.

3.4.13.1. Contractor shall ensure the following tasks are accomplished:
- Provide logistical support to Communications Security (COMSEC), Emissions Security (EMSEC), and Computer Security (COMPUSEC) programs.
- Provide guidance and support to system administrators/CSCs.
- Provide project management support on SIPR related tasks.
- Provide support to AFRC GCCS PMO and AFRC leadership in budget planning.

3.4.13.2. Qualifications:
- Technical skills and operational experience in AFRC GCCS-SIPR.

- Technical experience in VMware virtual environments.
- Technical experience in Windows-based workstation and server operating systems.

3.4.13.3. Certifications:
- 8570 certification required; IAT Level 2 certification is required.

3.4.13.4. Deliverables:
- New technology research briefings/reports, as required. **(CDRL A011)**
- Status reports of task activities, as required. **(CDRL A009)**

3.4.14. Print Management Support – (SC). AFRC has 20 print servers supporting the HQ AFRC user population (1,900 users) utilizing approximately 180 multi-function printers (predominately Lexmark).

3.4.14.1. Contractor shall ensure the following tasks are accomplished:
- Coordinate with bases and HQ CFP on print server application management.
- Utilize centralized capabilities to manage and enforce compliance of printers across command.
- Make recommendations for implementing the command's efforts for overall AFRC print server policies and management.
- Plan and implement enterprise print server management, security, configuration control for AFRCs AFNet print servers.
- Make recommendations on new printer technology for devices, management software/processes, configuration controls and methods.

3.4.14.2. Qualifications:
- Technical experience utilizing print management systems.
- Technical experience with CAC release.
- Technical experience utilizing PowerShell.
- Technical experience with Microsoft Windows Server 2008R2 or newer.

3.4.14.3. Certifications:
- 8570 certification required; IAT Level 2 certification is required.

3.4.14.4. Deliverables:
- Trend and performance analysis reports (e.g., metric of servers, print devices, and utilization rates), as required. **(CDRL A010)**
- New technology research briefings/reports, as required. **(CDRL A011)**
- Status reports of task activities, as required. **(CDRL A009)**

3.4.15. HQ AFRC and AFRC Host Base PKI/LRA Support – (SC):

3.4.15.1. Contractor shall ensure the following tasks are accomplished:

- Provide physical presence to issue token to users.
- Manage request and delivery of SIPR Alternate Tokens.
- Follow and implement processes for Alt Token issuance as governed by the Air Force Public Key Infrastructure (PKI) System Program Office.
- Perform as the Local Registration Authority (LRA) to include issuing software certificates to support organizational email and admin accounts.
- Interface with AFNet organizations and Air Force Directory Services (AFDS), AF PKI SPO, and others to resolve issues.
- Maintain an LRA database including installing, upgrading and configuring hardware/software used to support the database; performs system/database backups.
- Complete the AF PKI/LRA Course within 90 calendar days from contract award.
- For HQ LRA Only: Provide support to the AFRC LRAs.

3.4.15.2. Qualifications:
- Require knowledge of Public Key Infrastructure (PKI).

3.4.15.3. Certifications:
- 8570 certification required; IAT Level 2 certification is required.

3.4.15.4. Deliverables:
- Trend and performance analysis reports (e.g., metric of token count and token breakage by users and organizations), as required. **(CDRL A010)**
- New technology research briefings/reports, as required. **(CDRL A011)**
- Status reports of task activities, as required. **(CDRL A009)**

3.4.16. <u>AFRC Installation Warning System (IWS) Alerts Emergency Management Support – (SC)</u>. HQ AFRC supports AFRC implementation of AtHoc's Installation Warning System (IWS) Alerts Emergency Management System and provides support to approximately 70,000 AFRC personnel who are using the IWS alerts software. This currently includes supports of two (2) databases and six (6) application servers (currently) located at Robins AFB, GA and Dobbins ARB, GA.

3.4.16.1. Contractor shall accomplish the following tasks:
- Reset Wing Operator/Administrator passwords.
- Respond to and remediate trouble calls from AFRC users and works trouble/resolution issues with the appropriate Wing, AtHoc Help Desk, and/or AtHoc Engineer.
- Coordinate with AFRC/A6X for programmatic issues.
- Assist users in generating reports and queries to assist in tracking alert status.

3.4.16.2. Qualifications:
- Technical experience utilizing PowerShell.
- Technical experience with Microsoft Windows Server 2008R2 or newer.

3.4.16.3. Certifications:

- 8570 certification required; IAT Level 2 certification is required.

3.4.16.4. Deliverables:

- Trend and performance analysis reports (e.g., metric database accuracy by user), as required. **(CDRL A010)**
- New technology research briefings/reports, as required. **(CDRL A011)**
- Status reports of task activities, as required. **(CDRL A009)**

3.4.17. Server Support – (SC). HQ AFRC currently supports approximately 50 virtual and physical servers which must be maintained daily to ensure they support routine operations and meet required security controls.

3.4.17.1. Server Management Support – (SC). HQ AFRC currently supports 2 FAX servers, 2 Internet Protocol Television (IPTV) servers, 5 EA servers, and 12 general servers.

3.4.17.1.1. Contractor shall ensure the following tasks are accomplished:

- Serve as AFRC's IPTV manager:
  - Recommend overall AFRC IPTV policies, management and support.
  - Implement enterprise IPTV management, security, configuration control.
  - Coordinate, test, document, evaluate and implement new IPTV technology.
- Serve as AFRC's FAX manager:
  - Recommend overall AFRC FAX policies, management and support.
  - Implement enterprise FAX server management, security, configuration control.
  - Coordinate, test, document, evaluate and implement new FAX technology.
- Support additional 12 servers/services that are general in nature.
- Provide user account maintenance and support.
- Provide recommendations to return sites to an operational status.
- Assist the HQ AFRC ISSM with IA and C&A.
- Serve as EA Server Administrator**.**
  - Perform Tier 3 support for EA Server issues; troubleshoot server and network issues with Government personnel.
  - Perform server maintenance and patching to include server OS updates, security patches, and any other Government required patches.
  - Maintain EA Server Security Technical Implementation Guide (STIG) compliance and any other required information assurance actions.
  - Perform maintenance and configuration of IIS and SQL Server as needed for EA server support.
  - Troubleshoot server and network issues impacting the EA technical environment with Government personnel.

3.4.17.1.2. Qualifications:

- Technical experience utilizing PowerShell.
- Technical experience with Microsoft Windows Server 2008R2 or newer.
- Significant experience as a MS server administrator

3.4.17.1.3. Certifications:

- 8570 certification required; IAT Level 2 certification is required.

3.4.17.1.4. Deliverables:

- New technology research briefings/reports, as required. **(CDRL A011)**
- Status reports of task activities, as required. **(CDRL A009)**

3.4.17.2. SharePoint Server Support – (SCXP). Responsible for daily routine operations and maintenance of SharePoint (SP) servers. Supports and provides Central Administration duties, configuring SharePoint, patching and updating software to include SharePoint and the OS.

3.4.17.2.1. Contractor shall accomplish the following tasks:

- Coordinate with SP architecture as focal point for problem resolution and is the primary POC for Tier 2 issues.
- Develop, plan, design, test, implement, upgrade and manage the internal/external SharePoint sites.
- Coordinate, document, test, validate, and deploy new technology.
- Perform daily Central Admin tasks.
- Configure hardware for optimal performance.
- Patch and update all software, as required.
- Ensure high availability for all services; 24/7 availability with 99.99% uptime.

3.4.17.2.2. Qualifications:

- Significant experience with MS SharePoint Administration with the most recent 3 years in SharePoint 2013.
- Knowledge of SharePoint Architecture and functionality and related technologies (Win server admin, win architecture, SQL server, IIS, Active directory, SSL, Kerberos, F5, ISA, BI, Enterprise Search, BCS, ULS Logs, SQL Server Reporting Services (SSRS), Microsoft Office.
- Knowledge of Central Admin, SharePoint Services, SharePoint Object Model, Work Flow, Info Path, Form Services, KPIs, BDC, Records Management, Business Intelligence, Enterprise Search, Excel Services, SharePoint security model, timer jobs, ULS logs, and Microsoft SharePoint 2013 and above.

3.4.17.2.3. Certifications:

- 8570 certification required; IAT Level 2 certification is required.
- MCSE certification.

3.4.17.2.4. Deliverables:

- System uptime metrics, monthly. **(CDRL A018)**
- Site metrics, as required. **(CDRL A012)**
- User metrics, as required. **(CDRL A012)**
- Configuration control documentation of system changes, as required. **(CDRL A019)**

3.4.17.3. <u>SOCE Server Support – (SCXP)</u>. The SOCE contains 32 servers, both virtual and physical. These servers must be maintained daily to ensure they meet required security controls.

3.4.17.3.1. Contractor shall ensure the following tasks are accomplished:

- Patch and maintain all SOCE servers and appliances.
- Provide technical solutions and escalated support for technical issues.
- Maintain STIG compliance on hardware and software.
- Provide configuration management for the SOCE development, testing and production environments.
- Application maintenance and configuration (IIS, MS SQL Servers, Layer 7, PingFederate, etc.).
- Provide Tier 3 support for SOCE NIPR, SIPR, and all service capabilities.
- Assist HQ AFRC ISSM with IA and C&A requirements.
- Obtain and maintain all applicable IT compliance for SOCE (e.g., FISMA, NDAA, etc.).

3.4.17.3.2. Qualifications

- Significant experience with MS Windows Server 2012 sustainment experience.
- Technical experience with MS PowerShell.
- Technical experience with Layer 7 and PingFederate appliances.
- Technical experience with MS Networking Load Balancing and virtual environments.
- Technical experience with C&A, RMF procedures with proven abilities to create successful packages.

3.4.17.3.3. Certifications

- 8570 certification required; IAT Level 3 certification is required.

3.4.17.3.4. Deliverables

- Configuration management documentation, as required. **(CDRL A019)**
- SOCE Uptime Metrics, monthly. **(CDRL A020)**

3.5. <u>Cyber Compliance Support – (SC)</u>. HQ AFRC provides an AFRC-wide focused, "always ready" posture for successfully completing a Command Cyber Readiness Inspections (CCRI). Supports critical, MAJCOM-wide security-based functions required to always be resourced.

3.5.1. Enterprise Scripting Support – (SC).

3.5.1.1. Contractor shall ensure the following tasks are accomplished:

- Establish and execute scripts, plans and executes strategies to comply with the approximately 40 Cyber tasking orders monthly.
- Establish and execute scripts, plans and executes strategies to remediate the approximately 240,000 vulnerabilities (on average) across the 25,000 workstations and 800 servers in AFRC.
- Educate and facilitate vulnerability management with PMO and non-PMO system owners to include sharing and executing scripts, if requested.
- Design and execute other methods, as required, to facilitate vulnerability management.
- Ensure NIPR/SIPR CAT vulnerabilities for each assigned server does not exceed AFRC, AF, DISA, or DoD vulnerability thresholds; must be ≤2.49 vulnerabilities per each assigned server.
- Server administrators will implement AF Maintenance Tasking Orders (MTOs), TCNOs, and CCOs by established deadlines with 95% compliance for MTOs; 100% compliance for TCNOs and CCOs. All non-compliant MTOs will be corrected within 5 days.
- Comply with CCRI evaluation criteria [e.g., STIGs and Computer Network Defense (CND) Directives] include these overarching categories:
    - Technology. Includes (not inclusive) infrastructure, Assured Compliance Assessment Solution (ACAS) scans, traditional security, wireless
    - CND Directives. US Cyber Command issued directive compliance (e.g., compares network admin accounts to 8570 certification tracking
    - Contributing Factors. More policy driven similar to self-inspection compliance
- Identify improvements for processes and procedures, and introduce automation to improve.
- Participate in design and implementation activities emphasizing supportability, maintainability, scalability, performance and overall quality.
- Support innovative cloud-based solutions from the virtualization layer up through the software-defined and cloud management platform stacks.
- Establish a near real-time, AFRC-wide comprehensive single screen presentation (e.g., single pane of glass or dashboard) to facilitate CCRI preparedness, situational awareness, remediation actions, better understanding of issues in the operational environment, etc.
    - Provide drill-down capabilities in the presentations, to include by-base and by function drill-down capability according to CCRI criteria.
- Implement and maintain thorough vulnerability management programs to include creating/executing scripts (preference to PowerShell) to comply with tasking orders, remediation of client and server vulnerabilities, and general purpose scripts

- Establish and maintain visibility and tracking of compliance with CCRI evaluation criteria

3.5.1.2. Qualifications/Experience:
- Technical experience in AFNet.
- Technical experience utilizing PowerShell.
- Technical experience remediating Windows Server 2008RS and newer.
- Technical experience utilizing SCCM.
- Technical experience remediating MS-based Windows workstations.

3.5.1.3. Certifications:
- 8570 certification required; IAT Level 3 certification is required.

3.5.1.4. Deliverables:
- New technology research briefings/reports, as required. **(CDRL A011)**
- Status reports of task activities, as required. **(CDRL A009)**
- Trend and performance analysis reports (e.g., server and workstation vulnerabilities for AFRC), as required. **(CDRL A010)**

3.5.2. <u>Enterprise Compliance Support – (SC)</u>.

3.5.2.1. Contractor shall ensure the following tasks are accomplished:
- Serve as an ACAS administrator; run scans and reports; facilitate correcting permissions, settings, and other requirements to maintain DISA/AF vulnerability compliance.
- Execute scripts, plans and strategies to remediate the approximately 240,000 vulnerabilities (on average) across the 25,000 workstations and 800 servers in AFRC.
- Educate and facilitate vulnerability management with PMO and non-PMO system owners to include sharing and executing scripts, if requested.
- Design and execute other methods, as required, to facilitate vulnerability management.
- Comply with CCRI evaluation criteria [e.g., STIGs and Computer Network Defense (CND) Directives] include these overarching categories:
  - <u>Technology</u>. Includes (not inclusive) infrastructure, Assured Compliance Assessment Solution (ACAS) scans, traditional security, wireless
  - <u>CND Directives</u>. US Cyber Command issued directive compliance (e.g., compares network admin accounts to 8570 certification tracking
  - <u>Contributing Factors</u>. More policy driven similar to self-inspection compliance
- Establish a near real-time, AFRC-wide comprehensive single screen presentation (e.g., single pane of glass or dashboard) to facilitate CCRI preparedness, situational awareness, remediation actions, better understanding of issues in the operational environment, etc.

    - Provide drill-down capabilities in the presentations, to include by-base and by function drill-down capability according to CCRI criteria.
- Establish and maintain visibility and tracking of compliance with CCRI evaluation criteria

3.5.2.2. Qualifications/Experience:
- Technical experience in AFNet.
- Technical experience utilizing PowerShell.
- Technical experience remediating Windows Server 2008RS and newer.
- Technical experience utilizing SCCM.
- Technical experience remediating MS-based Windows workstations.

3.5.2.3. Certifications:
- 8570 certification required; IAT Level 3 certification is required.

3.5.2.4. Deliverables:
- New technology research briefings/reports, as required. **(CDRL A011)**
- Status reports of task activities, as required. **(CDRL A009)**
- Trend and performance analysis reports (e.g., server and workstation vulnerabilities for AFRC), as required. **(CDRL A010)**

3.6. <u>Information Assurance (IA), Computer Security (COMPUSEC), Certification and Accreditation (C&A) Support – (SC)</u>. HQ AFRC/A6 is responsible for the Wing Cybersecurity Office (WCO) function. The HQ AFRC WCO function is the Chief, Networks System Division's authority and focal point responsible for developing and maintaining the HQ AFRC cybersecurity program. The HQ AFRC WCO will address all cybersecurity requirements at HQ AFRC for IT under the control of the HQ AFRC/SC. The basic services include, but are not limited to the following:

3.6.1. Contractor shall ensure the following tasks are accomplished:
- Serve as HQ AFRC Information Systems Security Manager (ISSM).
    - Ensure HQ AFRC/A6 packages are converted from DoD Information Assurance Certification and Accreditation Process (DIACAP) to Risk Management Framework (RMF).
    - Maintain the TEMPEST Program at HQ AFRC/A6 to address all TEMPEST requirements.
- Develop, oversee, and maintain HQ AFRC Directorates and Special Staff Cybersecurity Program IAW AFI 33-200.
- Develop and maintain HQ AFRC/A6 enclave C&A packages.
- Oversee all HQ AFRC/A6 C&A packages; maintain situational awareness and initiate actions to improve or restore the cybersecurity posture as well as conduct annual security reviews of all IA controls and a test of selected IA controls IAW AFI 33-210.
- Provide data for FISMA compliance.

- Establish and maintain a COMPUSEC Program for HQ AFRC; address all AF COMPUSEC requirements IAW AFMAN 33-282;
  - Implement and enforce all AF cybersecurity policies, procedures, and countermeasures.
- Serve as the DoD 8570 Program Manager for HQ AFRC/A6; track and manage cybersecurity positions assigned which include, but are not limited to: system ISSMs/ISSOs assigned by PM's, COMSEC Account Managers (CAMs), COMSEC Responsible Officers (CROs), Cybersecurity Liaisons, Privileged Users, and Secure Voice Responsible Officers (SVROs) IAW AFMAN 33-285.
- Serve as liaison between HQ AFRC/A6 and Robins AFB COMSEC Manager.
- Complete DoD C&A Course within 180 days of contract award.
- Complete Air Force ISSM Course within 180 days of contract award.

3.6.2. Qualifications:
- Technical experience with the AF Information Assurance (IA) Program.
- Technical experience with the C&A process.

3.6.3. Certifications:
- 8570 certification required; IAM Level 2 certification is required (e.g., CISM or CISSP).

3.6.4. Deliverables:
- Artifacts required for authority to operate and other C&A requirements, as required. **(CDRL A021)**
- Status reports of task activities, as required. **(CDRL A009)**
- Trend and performance analysis reports, as required. **(CDRL A010)**

3.7. HQ AFRC and AFRC Host Base Communications Services Support. AFRC provides Tier 1 and touch labor support for user devices (workstations, laptops, tablets, zero clients, and mobile), printers, IPTV display boxes, applications on the user devices (including virtual instances of user profiles), and other hardware/software issues requiring remediation through remote assistance or physical presence. Communication services provides support activities to the user populations and devices in Table 4.

3.7.1. HQ AFRC and AFRC Host Base Communications Focal Point (CFP) Support – (SC/Bases):

3.7.1.1. Contractor shall ensure the following tasks are accomplished:
- Meet TO 00-33A-1001 requirements (and other instructions, as implemented).
- Remediate vulnerabilities on assigned hardware and software.
- Track Preventative Maintenance Inspections (PMIs) of required devices, servers, etc., using Integrated Maintenance Database System (IMDS), or other HQ AFRC designated system.

- Track local tickets in Remedy—both directly assigned to HQ AFRC/AFRC host base and HQ AFRC/AFRC host base user tickets assigned to another organization's queue.
- Utilize TBA system to manage training.
- Assign, monitor, and manage workload in the Client Support Center (CSC).
- Manage, review, disseminate, and implement AFNet NOTAMs/OPORDs/orders
- Monitor network status (currently via SCOM).
- Complete CFP Self-Assessments in Management Internal Control Toolset (MICT).
- Coordinate with PMOs that have systems running at HQ AFRC and AFRC host base for vulnerability remediation, C&A documentation and other support requirements (including DISA/AF driven).
- Ensure NIPR/SIPR CAT vulnerabilities for each assigned server does not exceed AFRC, AF, DISA, or DoD vulnerability thresholds; must be ≤2.49 vulnerabilities per each assigned server.
- Server administrators will implement AF Maintenance Tasking Orders (MTOs), TCNOs, and CCOs by established deadlines with 95% compliance for MTOs; 100% compliance for TCNOs and CCOs. All non-compliant MTOs will be corrected within 5 days.
- At HQ AFRC only:
  - Assign and monitor Tier 2 user issues documented in Remedy to Directory Services, Virtualization Management, Cyber Transport, Storage and Backup, Print server issues, Messaging, Mobile and Mobile Application back shops.
  - Act as CFP Functional Area Manager and provides CFP guidance to AFRC host bases.

Provide support for incident management.

3.7.1.2. Qualifications:

- Technical experience in AFNet.
- Technical experience utilizing PowerShell.
- Technical experience utilizing Remedy.
- Technical experience remediating MS-based Windows workstations.

3.7.1.3. Certifications:

- 8570 certification required; IAT Level 2 certification is required.

3.7.1.4. Deliverables:

- New technology research briefings/reports, as required. **(CDRL A011)**
- Status reports of task activities, as required. **(CDRL A009)**
- Trend and performance analysis reports, as required. **(CDRL A010)**
- CFP specific dashboards for situational awareness and decision-making utilization. **(CDRL A022)**

3.7.2. HQ AFRC and AFRC Host Base Client Support Centers (CSCs) Support – (SC):

3.7.2.1. Contractor shall ensure the following tasks are accomplished::

- Function as focal point for user and workstation problem resolution. Provide end-to-end ownership of incidents with actual or potential impact to operations.
- Create and maintain a central repository for technical advice and solutions for network systems, (CST/CFP share drive, Tier 0, etc.), software applications assistance, automatic data processing support, hardware exchange, and repair service support.
- Assist with reporting network performance metrics using Remedy Action Reporting System.
- Utilize Remedy to enter, document, track, coordinate, route, resolve, and close user ticket issues.
- Coordinate with AFNet Mission Assurance Center (AMAC), ESU, HQ AFRC workcenters, other AFRC host bases, and the AFRC/MCCC to work all user issues.
- Work with HQ software license manager to prevent unlicensed software from being used on the network.
- Administer cloud-related components and operational management tools.
- Maintain cloud user access roles, presentation of applications and automation workflows.
- Support requirements to configure and implement any required cloud integration with other applications, automation monitoring and automated event/ incident remediation wherever possible and appropriate.
- Manage and maintain VMs and virtualization related technologies, including configuration management tools.
- Image, reimage, work-assist tech refresh for workstations, printer support, hand-held mobile devices, etc.
- Support workstation types that include: desktops, laptops, tablets, zero clients, mobile devices (including smartphones and iPads), tablets, etc.
- Support Lync-Enterprise/Skype for Business user capabilities and functionality.
- Assist in evaluation, testing, documenting, deploying new user-base technology.
- Function as an equipment custodian, as required.
- Assist with local user training, performs initial fault assessment and resolution.
- Work, coordinate, document, resolve, and close trouble tickets and coordinate activities with CSTs in the CSC.
- Manage the Remedy queues supporting the local users (e.g., at HQ or respective base).
- Support will include those IA duties, as required by AFNet.
- Utilize Remedy Management System (RMS) to maintain historical database of reported problems and associated events.
- Provide Tier 0 and 1 support includes support to NIPR/SIPR services.
- Remediate vulnerabilities on assigned systems and report in AF designated systems (e.g., ACT).

- Provide an "always ready" posture for successfully completing a Command Cyber Readiness Inspections (CCRIs) for Tier 1, user-facing vulnerabilities.
- HQ AFRC only:
  - CSC will ensure NIPR/SIPR CAT vulnerabilities for each workstation does not exceed AFRC, AF, DISA, or DoD vulnerability thresholds; must be <2.49 vulnerabilities per workstation.
  - CSC will maintain customer satisfaction levels specified with 85% Customer Satisfaction.
  - Provide Client Support Centers (CSCs) Support; by the first business day of the week, ≤50 unresolved tickets in the queue for the previous week.
  - Provide Client Support Centers (CSCs) Support; ensure ≤85% of all tickets that were closed during the week were not open longer than 14 days.

3.7.2.2. Qualifications:

- Technical experience utilizing PowerShell.
- Technical experience remediating MS-based Windows workstations.

3.7.2.3. Certifications:

- 8570 certification required; IAT Level 2 certification is required.

3.7.2.4. Deliverables:

- New technology research briefings/reports, as required. **(CDRL A011)**
- Status reports of task activities (e.g., calls received, number of trouble tickets submitted, average resolution time, listing of technical bulletins and information guides issued.), as required. **(CDRL A009)**
- Trend and performance analysis reports, as required. **(CDRL A010)**

3.7.3. **Server Support – (All Bases)**. Each AFRC host base has NIPR and SIPR servers supporting the missions at those bases. The NIPR and SIPR environments utilize physical servers and a VMware virtual environment with storage and backup capabilities.

3.7.3.1. Contractor shall accomplish the following tasks:

- Support base-centric servers supporting the base user population. Services/servers include:
  - IPTV
  - Print Servers
  - AtHoc
  - DHCP
  - File storage and backup services
  - VMware suites and virtual services
  - Authentication servers (currently Cisco ACS)
- Perform support for server issues; troubleshoot server and network issues with Government personnel.

- Perform server maintenance and patching to include server OS updates, security patches, and any other Government required patches.
- Maintain server Security Technical Implementation Guide (STIG) compliance and any other required information assurance actions.
- Perform maintenance and configuration of IIS and SQL Server as needed for server support.
- Troubleshoot server and network issues impacting the technical environment with Government personnel.
- Configure hardware for optimal performance.
- Ensure NIPR/SIPR CAT vulnerabilities for each assigned server does not exceed AFRC, AF, DISA, or DoD vulnerability thresholds; must be ≤2.49 vulnerabilities per each assigned server.
- Server administrators will implement AF Maintenance Tasking Orders (MTOs), TCNOs, and CCOs by established deadlines with 95% compliance for MTOs; 100% compliance for TCNOs and CCOs. All non-compliant MTOs will be corrected within 5 days.

3.7.3.2. Qualifications:
- Technical experience in AFRC and AFNet.
- Technical experience utilizing PowerShell.
- Technical experience remediating Windows Server 2008RS and newer.

3.7.3.3. Certifications:
- 8570 certification required; IAT Level 2 certification is required.

3.7.3.4. Deliverables:
- Status reports of task activities, as required. **(CDRL A009)**
- New technology research briefings/reports, as required. **(CDRL A011)**
- Trend and performance analysis reports. **(CDRL A010)**

3.8. Video Teleconferencing. (See Table 3). The HQ AFRC VTC environment consists of 8 VTC suites using IP-based (with ISDN as an alternate) connectivity. On a weekly basis, approximately 15-30 VTC sessions and 100-125 conference room events occur. Additionally, the VTC hub located at HQ AFRC will provide VTC hosting services to AFRC, AFRC host bases, and AFRC tenants expanding local support to users throughout the command.

3.8.1. **VTC System Engineering Support – (SC)**.

3.8.1.1. Contractor shall ensure the following tasks are accomplished:
- Serve as the Video Teleconferencing (VTC) hub manager for VTC hub (located at HQ AFRC) supporting VTC session hosting across AFRC.
- Program and integrate Crestron products.
- Schedule, coordinate and facilitate VTC requests/sessions.

- Maintain VTC Account Database.
- Track, document and brief management on VTC utilization trends.
- Maintain and update web-based VTC schedule.
- Provide access list for room supporting VTC hub infrastructure equipment.
- Provide maintenance and/or troubleshooting support for legacy ISDN issues affecting VTC hub services.
- Maintain inventory control.
- Provide enterprise installation support, technical documentation, ongoing troubleshooting and maintenance, and on-site training support for VTC services.
- Act as enterprise VTC network maintenance focal point; receives and responds to alerts from VTC users/network VTC systems.
- Coordinate with appropriate vendors for maintenance support.
- Configure systems, communications devices, and peripheral equipment.
- Develop and maintain AFRC VTC Directory.
- Install, configure, and upgrade network hardware/software.
- Develop training materials, and train on-site personnel in the proper use of the VTC-Audio/Visual (A/V) hardware/software.
- Support on-site installations from maintenance vendor.
- Perform safe custodian duties.
- Manage secure key material for classified VTC equipment.
- Integrate VTCs and A/V equipment with 3rd party communications solutions (e.g., Creston).
- Provide monthly VTC usage reports with a 99% success rate of VTC sessions per month. **(CDRL A010)**
- Server administrators will implement AF Maintenance Tasking Orders (MTOs), TCNOs, and CCOs by established deadlines with 95% compliance for MTOs; 100% compliance for TCNOs and CCOs. All non-compliant MTOs will be corrected within 5 days.
- Ensure NIPR/SIPR CAT vulnerabilities for each assigned server does not exceed AFRC, AF, DISA, or DoD vulnerability thresholds; must be $\leq$2.49 vulnerabilities per each assigned server.

3.8.1.2. Qualifications:

- Significant experience with Enterprise VTC service delivery.
- Significant experience administering and configuring VTCs and A/V suites.
- Experience engineering VTC over IP.
- Knowledge of Crestron products, integration, and programming.
- Knowledge of various A/V technologies.
- Knowledge of VTC technologies and common architecture equipment (e.g., Cisco, Codian).
- Knowledge of multicast on desktops (streaming audio/video), audio conferencing, point-to-point, and multipoint video conferencing.
- Knowledge of AF network architecture and security including:

- ATO changes and considerations.
- JITC certifications.
- APL / UC.
- TEMPEST and EMSEC standards.

3.8.1.3. Certifications:

- 8570 certification required, as required; IAT Level 2 certification is required.

3.8.1.4. Deliverables:

- Status reports of task activities, as required. **(CDRL A009)**
- New technology research briefings/reports, as required. **(CDRL A011)**
- Trend and performance analysis reports. **(CDRL A010)**

3.8.2. <u>VTC Operations Center Presentation Support – (SC)</u>:

3.8.2.1. Contractor shall ensure the following tasks are accomplished:

- Schedule, coordinate, facilitate, and set up VTC requests/sessions both secure and un-Secure
- Provide Senior-level presentation support for 8 HQ AFRC VTC-enabled conference rooms at various locations around the base.
- Coordinate presentation requirements for conference room users, presents PowerPoint and/or other presentation support through use of multimedia systems in these rooms.
- Provide technical support to customers on presentation capabilities and requirements for the conference rooms.
- Assist in scheduling of rooms for presentation support.
- Assist with setup of VTC call sessions on HQ AFRC VTC hub.
- Conduct basic trouble shooting, and coordinate with VTC Operations Chief on any issues which require resolution; includes testing with other AF units.
- Configure systems, multimedia devices and peripheral equipment.
- Support on-site maintenance from vendors.
- Serve as equipment custodian for all installed equipment in 8 HQ AFRC VTC-enabled conference rooms.

3.8.2.2. Qualifications:

- Knowledge of various AV technologies and software.
- Knowledge of Cisco Telepresence devices.
- Experience with Microsoft Office (Organizational Mailboxes and Calendars).
- Knowledge of GVS scheduling.
- Knowledge of ISDN and IP based conferencing.

3.8.2.3. Certifications:

- None required.

3.8.2.4. Deliverables:

- Status reports of task activities, as required. **(CDRL A009)**
- New technology research briefings/reports, as required. **(CDRL A011)**
- Trend and performance analysis reports. **(CDRL A010)**

3.8.3. HQ USAF/RE VTC Facilitator Support.

3.8.3.1. Contractor shall ensure the following tasks are accomplished:

- Provide video conferencing support to Headquarters United States Air Force, Office of Reserve Affairs (HQ USAF/RE).
- Serve as VTC configuration manager, web developer, and facilitator for HQ USAF/RE.
- Schedule, coordinate, facilitate, and set up VTC requests/sessions, both secure and un-Secure.
- Maintain VTC account information.
- Track, document, and brief management on VTC utilization trends.
- Provide daily VTC availability reports to appropriated agencies.
- Provide installation support, technical documentation, ongoing troubleshooting and maintenance, and on-site training support for desktop VTC services.
- Act as centralized VTC network maintenance focal point for the HQ USAF/RE VTC system, receive and respond to alerts from VTC users/network VTC systems.
- Conduct basic troubleshooting, and coordinate with HQ AFRC VTC Operations for maintenance support. Configure VTC systems, related communications devices, and peripheral equipment to include testing with other AF units.
- Install, configure, and upgrade network hardware/software.
- Set up VTC sessions, to include bridging of VTC calls through the AFRC VTC Operations Office at Robins AFB, GA.
- Develop training materials, and train on-site personnel in the proper use of the VTC-A/V hardware/ software.
- Perform on-site installations, configure the hardware and software for the appropriate telecommunications service, and test for connectivity and interoperability.
- Analyze existing requirements and prepare specifications for hardware/software acquisitions and/or upgrades.
- Build specialized interconnecting cables.
- Provide presentation support, as required.
- Provide monthly VTC usage reports with a 99% success rate of VTC sessions per month. **(CDRL A010)**

3.8.3.2. Qualifications:

- Knowledge of various AV technologies and software.
- Knowledge of with Cisco Telepresence devices.

- Experience with Microsoft Office (Organizational Mailboxes and Calendars).
- Knowledge of with GVS scheduling.
- Knowledge of ISDN and IP based conferencing.
- Experience with multicast on desktops (streaming audio/video), audio conferencing, point-to-point, and multipoint video conferencing.

3.8.3.3. Certifications:
- None required.

3.8.3.4. Deliverables:
- Status reports of task activities, as required. **(CDRL A009)**
- New technology research briefings/reports, as required. **(CDRL A011)**
- Trend and performance analysis reports. **(CDRL A010)**

3.8.4. Enterprise Microsoft SharePoint (SP) Farm Support. AFRC hosts an enterprise level SharePoint 2013 farm on both NIPR and SIPR. The NIPR farm currently provides services to approximately 70,000 users (internal and external), with a potential for an increase in user base. Site Collections counts are approximately 110 with 2300 sub-sites. The farms consist of 26 virtual servers and 4 physical servers, providing production, staging, and test environments. Two types of load balancers are in place to support different user traffic, F5 and MS Threat Management Gateway (TMG) servers. AFRC also hosts a smaller scale farm on SIPR. All servers are running Windows server 2012 or higher, the SQL servers are running MS SQL 2012. SQL servers run in high availability mode to provide 24 hours-a-day/7 days a week (24/7) access and an uptime of 99.99%. Customer service levels ranging from Tier 1 thru Tier 3 are provided as part of Service Level Agreements (SLA) and Governances in place. Several custom solutions are deployed in both farms, with the potential for additional solutions, (Government and commercial solutions). SP team works closely with internal software development team to facilitate insuring proposed solutions meet farm architecture, engineering, and governance requirements. AFRC expects to use Infrastructure as a Service (IaaS) and Software as a Service (SaaS) as AFRC moves to a cloud based solution.

3.8.4.1. <u>SharePoint Architecture Support – (SCXP)</u>. HQ AFRC is responsible for planning, analysis, design and implementation/upgrades to current and future farm installations. Ongoing analysis should result in performance tuning for optimal use as the SP usage grows.

3.8.4.1.1. Contractor shall ensure the following tasks are accomplished:
- Plan, analyze, design and implement/upgrade to a cloud-based solution.
- Develop, plan, design, test, implement, upgrade, and manage the internal and external SharePoint sites (includes 2013 and future upgrades) supporting AFRC and its partners.
- Develop the overall website design and structure, monitor web site functionality, security, and integrity, troubleshoot and resolve problems, review, test, collect

and analyze website statistics, evaluate new web applications and provide technical advice to web content providers.
- Analyze AFRC's information architecture, maintain and configure organization taxonomies, site collections, policies, procedures, solutions.
- Coordinate with developers to install, debug, and maintain necessary code of assigned software.
- Troubleshoot and resolve Tier 3 issues with the SharePoint environment.
- Provide technical solutions and escalated support for technical issues.
- Plan, conduct and oversee the technical aspects of projects; coordinate the efforts of technical support staff in the performance of assigned projects.
- Analyze, design, and develop custom Business Intelligence (BI) solutions utilizing SQL Server Analysis and Reporting Services, integrated with SharePoint.
- Minimizes services, application, and system unscheduled downtime; 99% availability for the month with no more than 7 hours of downtime within contractor's control.
- Provides configuration control documentation of system changes; on-time delivery at 100% level (monthly).

3.8.4.1.2. Qualifications:
- Extensive experience with MS SharePoint Administration with the most recent 3 years in SharePoint 2013.
- Knowledge of SharePoint Architecture and functionality and a working knowledge of related technologies such as: Windows Server administration, Windows Architecture, SQL Server 20xx, Internet Information Server, Active Directory, Secure Socket Layer (SSL), Kerberos, ISA and Microsoft Office desktop application integration with SharePoint, F5, MS TMG.
- Knowledge of SharePoint Services, SharePoint Object Model, Work Flow, Info Path, Form Services, Key Performance Indicators (KPIs), Business Data Connectivity (BDC), Records Management, Business Intelligence, Enterprise Search, Excel Services, SharePoint security model, timer jobs, ULS logs, and Microsoft SharePoint 2013 and above.
- Knowledge of IaaS and SaaS cloud services.

3.8.4.1.3. Certifications:
- 8570 certification required; IAT Level 2 certification is required.
- Microsoft ® Certified Systems Engineer (MCSE) certification.

3.8.4.1.4. Deliverables:
- Pre- and post-environment change documentation, as required. **(CDRL A023)**
- Governance updates, as required. **(CDRL A024)**
- MS Visio Farm diagrams/network infrastructure as it applies to the SP farms, as required. **(CDRL A023)**

3.8.4.2. <u>SharePoint Site Support – (SCXP)</u>. AFRC utilizes a federated support model, where each site owner is responsible for maintaining their sites and sub-sites. SP Site Support provides the initial creation of the sites and assigns rights and privileges as required. SP Site Support provides Tier 1 customer support for user education and administration.

3.8.4.2.1. Contractor shall ensure the following tasks are accomplished:

- Coordinate with SP Engineering as focal point for problem resolution and is primary POC's for Tier 1 issues.
- Coordinate with user/customer community for content and site structures.
- Troubleshoot issues with SharePoint as well as issues with content delivery, site usage, etc.
- Facilitate the gathering and documentation of requirements from users to facilitate design.
- Assist in the set-up of global standards and controls for internal team and project sites and assist in the development of training for business users on SharePoint functionality.
- Utilize Remedy to process tickets.

3.8.4.2.2. Qualifications:

- Technical experience with MS SharePoint Site Collection Administration with most recent in SharePoint 2013.
- Knowledge of Central Admin, SharePoint Services, Work Flow, Info Path, Form Services, KPIs, BDC, Records Management, Business Intelligence, Enterprise Search, Excel Services, SharePoint security model, and Microsoft SharePoint 2013 and above.

3.8.4.2.3. Certifications:

- 8570 certification required; IAT Level2 certification is required.

3.8.4.2.4. Deliverables:

- Provides configuration control documentation of system changes, as required. **(CDRL A019)**

3.8.5. Service Oriented Cloud Environment (SOCE). The Air Force Reserve (AFR) Service Oriented Cloud Environment (SOCE) is a highly available environment that hosts Web Services that deliver end-to-end business solutions. For AFR, Service Oriented Architecture (SOA) provides a discipline by which authoritative data sources can be exposed, aggregated, and presented. AFR has selected a core set of technologies and has implemented a SOA environment. This environment is supported on both NIPR and SIPR, providing 24/7 access with a 99.99% uptime requirement.

3.8.5.1. **<u>SOCE Team Lead Support – (SCXP)</u>.** The service development processes could range from 2 months to over 2 years development time, depending on the

complexity of requirements. Project coordination supports the development team by providing leadership functions to support technical solution development, and an IT platform supporting these services, so that measurable services can be produced for potential SOCE solutions.

3.8.5.1.1. Contractor shall ensure the following tasks are accomplished:

- Coordinate the efforts of the SOCE team.
- Investigate and test new technologies.
- Participate in Analysis of Alternatives.
- Contribute to Command innovation strategy sessions.
- Provide monthly status reports.
- Provide ROMs for new requirements.
- Review Bounded User Requirements as presented through SDDP.
- Conduct SOCE working group meetings.
- Maintain and update, as needed, SOCE Governance.
- Implement authoritative data acquisition.

3.8.5.1.2. Qualifications:

- Significant experience as a SOA software development team lead.
- Knowledge of Service Development Delivery Process (SDDP) and Agile development processes.
- Technical experience with AF Enterprise Architecture artifacts.
- Significant experience with C# in .NET and LINQ to Entities.
- Significant experience with WCF web services.
- Significant experience with SOAP and REST.
- Significant experience with Web Services Description Language (WSDL).
- Significant experience understanding of web service data contracts.
- Significant experience with Microsoft .NET Web API.
- Significant experience with MS Visual Studio, IIS, MS Windows Server 2012.

3.8.5.1.3. Certifications:

- 8570 certification required; IASAE Level 2 certification is required.

3.8.5.1.4. Deliverables:

- SOCE Working Group slides, as required. **(CDRL A025)**
- ROM estimates for COA selections, as required. **(CDRL A026)**
- SOCE Governance updates, as required. **(CDRL A024)**
- MOU's and SLA's per requirement specifications, as required. **(CDRL A027)**
- Status reports, monthly. **(CDRL A009)**

3.8.5.2. <u>SOCE Database Administration Support - (SCXP)</u>. The SOCE solution provides for data integrity, eliminating null data, errors, formatting discrepancies, and redundant data. The solution ensures that data is cleansed, transformed to a useable

format, catalogued, and made available for use. It integrates seamlessly with the AFRC Enterprise Service Bus (ESB) using SOA industry standards. The SOCE solution is capable of consuming data from AFRC unique, AF, and DoD systems. The SOCE utilizes an Extract Translate and Load (ETL) capability to consume data from existing database technologies such as Oracle, SQL, Excel spreadsheets, etc., and transform and store data in a consistent format. In addition to supporting analytics, the data solution also contains a common reference data store which contains data frequently used by several/many consumers with the AFRC Enterprise.

3.8.5.2.1. Contractor shall ensure accomplishment of all tasks as described in para 3.4.4.1. and the following:

- Creates ETL scripts for new service capabilities.
- Sustains ETL for all current authoritative data sources.
- Designs, documents and implements new schemas.
- Provides data quality metrics.
- Administers all operational data stores (ODS).
- Administers all databases.
- Performs database tuning and configuration.
- Minimizes services, application, and system unscheduled downtime; 99% availability for the month with no more than 7 hours of downtime within contractor's control.

3.8.5.2.2. Qualifications:

- Significant technical experience with MS SQL Server DBA.
- Technical experience using MS Biztalk Server software.
- Knowledge of Microsoft .NET Web API.

3.8.5.2.3. Certifications:

- 8570 certification required; IASAE Level 2 certification is required.

3.8.5.2.4. Deliverables:

- Schema documentation, as required. **(CDRL A028)**
- Data accuracy reports, as required. **(CDRL A009)**

3.8.5.3. **SOCE Service Development Support – (SC)**. SOCE requires Data Exposure and Business services to be created which provide authorized consumers the capability to enable aggregating, joining, and querying of data. Orchestration services will be leveraged to introduce complex rules and workflows that may contain new business rules, exception handling, and transaction management features, involving a number of different application and data sources.

3.8.5.3.1. Contractor shall ensure the following tasks are accomplished:

- Sustain all existing service capabilities.
- Provide Service Development Life Cycle (SDLC) for all new service capabilities.

- Provide SOCE health metrics (NIPR/SIPR).
- Perform SOCE SharePoint site maintenance.
- Create SQL Server Reporting Services reports.
- Perform SQL Server Reporting Services site maintenance.
- Provide ARCGis sustainment, including software updates and software administration.
- Minimizes services, application, and system unscheduled downtime; 99% availability for the month with no more than 7 hours of downtime within contractor's control.

3.8.5.3.2. Qualifications

- Significant experience with C# in .NET and LINQ to Entities.
- Significant experience with WCF web services.
- Knowledge of SOAP and REST.
- Significant experience with Web Services Description Language (WSDL).
- Significant experience with of web service data contracts.
- Significant experience with T-SQL in MS SQL Server and SQL Server Management Studio.
- Significant experience with Microsoft .NET Web API.
- Significant experience with MS Visual Studio, IIS, MS Windows Server 2012.

3.8.5.3.3. Certifications

- 8570 certification required; IASAE Level 2 certification is required.

3.8.5.3.4. Deliverables:

- Detailed service documentation, as required. **(CDRL A030)**
- Service availability metrics, as required. **(CDRL A029)**
- SOCE health metrics, monthly. **(CDRL A029)**

3.9. Microsoft (MS) Dedicated and Premier Engineering Support – (SC) – (Labor Hour CLIN Only). HQ AFRC/A6 requires Microsoft Dedicated Support Engineer (DSE) and/or Premier Field Engineer (PFE) support to further AFRC strategic IT needs and to assist in resolution of complex problems. Examples of the types of support required include, but are not limited to: virtualization environments, Exchange Server, SQL Server, Active Directory, SharePoint, cloud capabilities, and other MS product installations/maturations requirements as they arise in both the NIPR/SIPR environment. This support would be on an as needed basis as defined by the Government, above and beyond the skills and capabilities typically available. Support will be billed on a labor hour basis (Labor Hour CLIN).

3.9.1. Contractor shall ensure the following tasks are accomplished:

- Provide operational support and troubleshooting of MS products with direct access and escalation paths to MS product groups.

- Provide access to MS technology and development centers, as required, to test, prototype and deploy vendor solutions thus reducing risk and decreasing "time to value" in solution development cycle.
- Aid in the design and development of systems, and redesign of existing systems based on best practice recommendations.
- Provide implementation recommendations of MS software solution sets to allow for reduction of operational costs.
- Provide support of custom configurations to meet AFRC unique mission requirements.

4. GENERAL INFORMATION:

4.1. Period of Performance. Performance shall commence at date specified in resultant contractual document for a one-year basic period with four (4) annual option periods, and a 6-month 'short option' in accordance with Option for Extension of Services clause FAR 52.217-8.

4.2. Place of Performance. The Contractor personnel shall perform at: HQ AFRC, Robins AFB, GA; HQ ARPC, Buckley AFB, CO; 919 CS, Duke Field, FL; SAF/RE, Pentagon, Washington DC; 301 FW, NAS-JRB Ft Worth, TX; 304 RS, Portland IAP, OR; 434 ARW, Grissom ARB, IN; 439 AW, Westover ARB, MA; 452 AW, March ARB, CA; 482 FW, Homestead ARB, FL; 910 AW, Youngstown ARB, OH, and 911 AW, Pittsburgh ARS, PA.

4.3. Program Support:

4.3.1. Post Award Meeting**.** The Contractor shall attend a one (1) day post award kick-off meeting convened and hosted by the AFRC/A6 COR. The post award conference will be held within two (2) weeks of contract award. The location will be a mutually agreed upon site to be determined after award. The Functional Commander, GSA CO and AFRC/A6 COR will participate with Contractor Representatives. The meeting will provide an orientation and overview of the contract scope, terms and conditions. The meeting will detail the roles and responsibilities of AFRC team members, QASP, performance evaluations, contract administration and contract closeout.

4.3.2 Phase-In Period. The contractor shall develop comprehensive procedures for phasing in contractor performance to the level prescribed and within the time allowed under the terms of this contract. The phase in period shall be 30 days.

4.3.2.1 During the phase-in period (30 days), the contractor shall prepare to assume full responsibility for all areas of operation in accordance with the terms and conditions of this contract. The contractor shall take all actions necessary for a smooth transition of the contracted operations. The Government will make all

facilities and equipment accessible to the contractor. During this period the contractor's management personnel will be permitted to observe functions on a non-interference basis, as approved by the CO.

4.3.2.2 The contractor shall recruit and hire necessary personnel; obtain all required certifications and clearances, including personnel security clearances; participate in joint inventories and sign for Government-furnished Property (GFP) as applicable; develop and submit any required deliverables; attend post-award meetings as required; and accomplish any necessary training to support the requirement of this contract.

4.3.3 Phase-Out Period. Prior to the completion of this contract (to include option periods), an observation period shall occur, at which time management personnel of the incoming workforce may observe operations and performance methods of the incumbent contractor. This will allow for orderly turnover of facilities, equipment, and records and will help to ensure continuity of service. The incumbent contractor shall not defer any requirements for the purpose of avoiding responsibility or of transferring such responsibility to the succeeding contractor. The incumbent contractor shall fully cooperate with the succeeding contractor and the Government. The phase out period shall be 30 days.

4.3.4. The Contractor shall participate in programmatic meetings, reviews, and briefings associated with this contract.

4.4. Key Personnel and Personnel Substitutions:

Key personnel are those personnel considered essential to successful contractor performance. Key personnel identified include:

- On-Site Program Manager (para 2.1.).
- Enterprise Architecture Support (para 2.9.1.).
- Network Infrastructure Engineering Support (3.4.11.)
- Enterprise Scripting Support (para 3.5.1.)
- VTC System Engineering Support (par 3.8.3.1.).
- SharePoint Architecture Support (para 3.8.4.1.)
- SOCE Team Lead Support (para 3.8.5.1.).

The Key Personnel shall be identified in the Contractor's quote and shall also identify requisite years of experience, certifications, credentials and education IAW the solicitation, Organizational Structure/Staffing Plan.

Names and phone numbers shall be provided, in writing, to the CO and COR upon award.

Government will review the initial and/or replacement of key contractor personnel. Key personnel on this contract shall not be replaced or reassigned without prior review by the Government.

Substitutions for other personnel may be made in task staffing under the following conditions:

- The Contractor shall notify the COR at least ten (10) working days before making changes.
- The Contractor shall provide personnel who meet the qualification/experience and certifications of the personnel being replaced.

4.5. Site Leads. This contract does not assume or require any hierarchical structure; however, it requires that a Contractor Site Lead shall be identified at each location in order for the Government to ensure a first-line of communications. At the supported locations outside of HQ AFRC (see Table 3), a Government Lead will be designated to interact with the Contractor Site Lead.

4.6. **Network Licensing and Certification**:

4.6.1. Network User Licensing Program. Contract personnel must all meet the same licensing requirements before access is permitted to network resources [as outlined in Air Force Instruction (AFI) 33-115, Vol II], *Licensing Network Users and Certifying Network Professionals*.

4.6.2. Network Professional Certification Program. Contractors requiring elevated network administrative rights will comply with the Department of Defense Directive DoDD 8570.1, *Information Assurance Training, Certification and Workforce Improvement Plan*, (aka 8570) and AFMAN 33-285 (to be replaced by DODD 8140, Cyberspace Workforce Management) certification process prior to working on this contract. Furthermore, all Contractors requiring elevated network administrative rights shall be required to maintain 8570 certification at all times as well as complete the Privileged Access Agreement (PAA) form. Unless otherwise indicated, all 8570 certifications will be to the Level 2; some tasks will require Level 3 certification. The level of certification is identified in each task.

4.7. Reimbursable Costs. Contractor shall submit an estimate to either the Government Program Manager or COR which is forwarded to the CO for approval. Contractor shall not begin performance prior to obtaining CO approval.

The Contractor shall ensure that reimbursable costs do not exceed awarded budgets.

4.8. Travel. The Contractor may be required to fulfill the requirements of this PWS via travel (e.g., site visits). The Contractor shall coordinate travel via ITSS with the AFRC/A6 COR and get GSA CO approval prior to commencement of travel. The Contractor shall provide the purpose of the travel, number of participants, location and estimated cost. The Contractor travel payment is limited to reasonable and allowable costs to the extent that they do not exceed on a daily basis the maximum per diem rates in

effect at the time of travel as set forth in the Government's Joint Travel Regulation (JTR), Volume 2 and allowable per FAR 31.205-46, *Travel Costs*. Non-emergency travel requests will be submitted for approval not less than 30 days prior to travel dates. Emergency requests will be handled on a case-by-case basis.

Locations and the duration of travel cannot be established at this time so a not-to-exceed travel budget will be established on this contract.

4.9. Training. Training of Contractor employees assigned to this contract shall be performed at the Contractor's own expense, with these exceptions:

The Government has given prior approval for training to meet special requirements that are peculiar to the environment and/or operations (e.g., new technology).

The Government will provide required training that is Air Force specific or unique applications to ensure contractor performance.

The Government will not authorize contractor employees to attend seminars, symposiums, or other similar conferences for Government specific training unless the COR certifies, and CO approves, that attendance is mandatory for the performance of the task requirements.

In the event that the Government has approved and paid for contractor employee training, reimbursement shall not be authorized for costs associated with re-training replacement individual(s) should the employee(s) terminate from this contract.

4.10. Use of Government Vehicles. Travel to and from work sites may be required to fulfill the requirements of this contract. Contractor may utilize Government vehicles in accordance with AFI 24-301.

4.11. Performance Criteria:

4.11.1. Hours of Work:

- Normal duty hours are from 7:00 AM to 4:00 PM, Monday through Friday, excluding federal holidays.
- Any variation must be negotiated and pre-approved by the Government.
- Flextime is acceptable and reporting time can be between the hours of 7:00-9:00 AM for 8 hours-a-day, Monday - Friday, except Government holidays, for each site (not including 30 to 60 minutes for lunch); however, Government personnel must be present during all hours of contractor operation.

- Telework/telecommuting is authorized on an exception basis and only as approved by the COR and CO.
- The Contractor shall support all Unit Training Assemblies (UTAs) or as directed by the COR.

4.11.2. Variance in Regular Hours for Emergency Workload Peaks:

- Occasional emergency workload peaks, or changes in Government priorities, may necessitate that the Contractor discusses workload priorities with the COR and request the approval of a variance in regularly scheduled hours.
- If the COR cannot rank the jobs in order to meet critical deadlines without affecting predetermined shift composition, the COR may approve a shift variance, if requested.
- This does not constitute an approval for extended hour's compensation. Rather, the Contractor shall realign the scheduling of personnel to preclude the necessity for extended hours compensation.

4.11.3. Overtime. The Contractor personnel may require overtime hours due to unanticipated, short deadline work. Overtime work means each hour of work in excess of eight (8) hours in a day or in excess of forty (40) hours in a work week that is officially required. The Contractor shall coordinate the request for overtime with the AFRC/A6 COR. Overtime shall be approved in advance by the AFRC/PKA CO in accordance with FAR 52.222-2, *Payment for Overtime Premiums,* as supplemented in the Air Force Federal Acquisition Regulation (AFFAR).

4.12. Contractor Recall. If "after hour's system failure" occurs, the Contractor shall provide fully qualified personnel, accessible by phone, to perform the unscheduled mission or emergency requirement. For unscheduled mission requirements, Contractor personnel shall respond within 15 minutes of the initial notification and be on-site within 1 hour after the initial response in order to perform services and satisfy unscheduled mission requirement. For planning purposes, all communication units will be authorized to generate "on-call" rosters of contractors to be contacted in the event an unscheduled mission or emergency requirement that may occur after duty hours. If a Contractor recall is required, the Government On-Site Lead will either request overtime and/or adjust the contractor's work schedule. Only the PCO or COR are authorized to approve overtime.

4.13. Inclement Weather. There will be times when inclement weather will impact a base and/or organization (e.g., snow storm, flooding, etc...) in such a way that it will become a safety concern. When this happens and the Wing/Base Commander closes a base, the Contractor shall adhere to all directives of the military installation. When it comes to pay issues for time and labor contractor support, the Contractor shall only bill the Government for hours worked.

4.14. Federal Holidays. The contract shall not have staff present at the Government installation facilities on federal holidays. The federal holidays observed are as follows:

New Year's Day, Martin Luther King's Birthday, President's Day, Memorial Day, Independence Day, Labor Day, Columbus Day, Veterans Day, Thanksgiving Day and Christmas Day.

4.15. Family, Energy Conservation, and Early Release Days. There will be days when the Government, MAJCOM, and/or Base Commander will direct Family Days, Energy Conservation Days, and/or early release days. When these days are identified, the Contractor is expected to work when the facilities are available for them to do so. Furthermore, the COR can inform contractors regarding the level of performance expected for the particular day(s), but may not direct the Contractor regarding whether or not to compensate employees if not required to work that day. The Service Contract Labor Standards does not require Contractor employees to be paid for time if they do not work. The Contractor may elect to grant employees the day off with pay, but there is no additional Government contract costs (wages for these hours are already in the contract cost). This contract specifies that in order for contractors to remain in place, they must have Government oversight in place.

4.16. Telecommuting. Telecommuting allows written pre-authorization by approving authority to allow contractors to work in an official capacity away from the official duty location. The alternate work locations must have the necessary tools and environment to enable Contractor employees to accomplish assigned duties. The Government will determine if telecommute requests will be allowed on a position-by-position basis.

4.16.1. Roles and Responsibilities. The COR shall approve all requests for telecommuting after coordination with the CO.

4.16.1.1. Immediate Supervisor. The On-Site Program Manager is responsible for:

- Recommending the telecommuting project to the approval authority.
- Preparing required documentation and obtaining any necessary signatures from the telecommuter.
- Ensuring project details (e.g., scope of work, deliverables, etc.) are mutually agreed upon before beginning work.
- Quality control of the telecommuter's completed product.
- Maintaining the original approved agreement.

4.16.1.2. Contractor. Contractors are responsible for identifying telecommuting equipment requirements to the On-Site Program Manager.

- Contractor should obtain the approval authority's concurrence before performing telecommuting that exceeds the agreed hours.
- The approval authority of the telecommuting agreement may terminate participation in telecommuting at any time.

4.16.2. Government Furnished Equipment (GFE)**.** Subject to AFI 33-200, *Information Assurance (IA) Management*, AFMAN 17-1203 Information Technology (IT) Asset Management (ITAM), Air Force Systems Security Instruction (AFSSI) 8502, *Computer Security*, and other prescribed rules and limitations, a Commander may approve the installation of Government-owned computers, computer software, and telecommunications equipment (hereafter referred to as equipment) in alternative work locations:

- The commander or designated representative retains ownership and control of all hardware, software, and data associated with, or generated by, Government-owned systems. The commander must account for equipment on a hand receipt and inventory annually. The commander must notify the Equipment Control Officer (ECO) of the relocation of the equipment (AFI 33-112). Any equipment not returned to the Government shall be paid for by the Contractor.
- Government equipment is FOR OFFICIAL USE ONLY (FOUO). Commanders may authorize installation, repair, and/or maintenance of equipment at their discretion and direction. The equipment is for authorized use by the contractor only.
- The Contractor agrees to protect any Government-owned equipment from damage, loss, theft and infection with computer viruses.
- Individual contractors are not authorized to install hardware or software on a Government system; only unit CSTs have that authority and only with the permission of their unit commander.
- Contractors must follow Report of Survey (ROS) procedures for damaged, lost, or stolen Government equipment (AFI 33-112 and AFMAN 17-1203 Information Technology (IT) Asset Management (ITAM).
- Government information must be protected from modification, destruction, or inappropriate release.
- Users of Government-provided telecommunications in alternative work locations are subject to the monitoring requirements of AFI 10-712, *Telecommunications Monitoring and Assessment Program (TMAP).*

4.16.3. Equipment Obligations**:**

- Contractors using Government owned equipment must sign an agreement outlining the required equipment, software, hardware, data, and telecommunication services.
- Contractors must ensure that software use conforms to all copyright law and any contractual agreements.
- If network connection is required at the alternate duty location, it shall be at the contractor's expense.
- If telecommuting requirements terminate, the Contractor must immediately return Government owned hardware, software, data, and cancel all telecommunication services that the Government provided. (AFI 23-111, *Management of Government*

Property in Possession of the Air Force (AFI 33-112, AFMAN 23-110, Volume 2, *USAF Supply Manual*, Part 13, Chapters 4 and 8,).

4.17. GOVERNMENT PROPERTY, FACILITIES, AND INFORMATION:

4.17.1. Government Property, Facilities, and Information to be Provided. Government property, facilities, and information to be provided include personnel with office space, supplies, computers, telephone communications, internet access, printers, and access to appropriate Government files, databases and common access cards for use in the performance of this requirement.

4.17.2. The Government shall provide laptops to facilitate non-duty hour remote administration capability. All laptops will be brought in and connected to the AF network for a 24 hour period at minimum, once every seven (7) duty days. The contractor shall not alter the configuration of the laptop in any way to include, the loading/removal of software, the loading/removal of accounts or the connection of devices that violate established DoD, Air Force or local security guidance. All laptops are subject to security scan upon COR request.

4.17.3. Installation Support:

4.17.3.1. The Government will provide the on-site Contractor personnel with office space, supplies, computers, telephone communications, internet access, printers, and access to appropriate Government files, databases and common access cards for use in the performance of this requirement. **Use is limited to official Government business related to the performance of the requirements in this contract.** The AFRC will provide routine scheduled preventive maintenance of AFRC equipment that remains under the control of the Government. Upon request by the Contractor to the AFRC/A6 COR, the AFRC COR will provide repairs of Government equipment provided as part of Installation Support.

4.17.3.2. The Government shall furnish property incidental to the place of performance (Ex: cubicle space, desk, chair, desktop computer, access to copier, fax and a networked printer. In addition, the Government shall provide telephone service consisting of Class 3 and Class 1, to include the Defense Switched Network (DSN). Telephone service classes are defined in AFI 33-145, 6 Sep 12, Voice Systems Management, Section B, Chap. 31. The contractor shall ensure use of all government provided equipment/facilities is limited to performance of contract related official Government business. Upon completion or termination of the contract or expiration of employee identification passes, the prime contractor shall ensure that all GFE to include base ID passes, desktop computer, laptop computers, peripherals, and other software/hardware is returned to the COR and each individual is processed through the directed Out-processing checklist.

4.17.4. Government System(s). The Government will provide Contractor personnel access to system(s) necessary to perform tasks under the contract/order. Upon

completion/termination of the contract/order or transfer/termination of Contractor personnel, the system account(s) will be closed.

4.18. Security and Privacy:

4.18.1. Overview. The Contractor shall comply with all applicable security regulations and directives identified herein and other security requirements as shown elsewhere in this contract.

- Work on this contract requires all employees to meet Secret eligibility requirements IAW DoD 5200.2-R.
- Personnel are required to read, store, process sensitive information and operate/program sensitive database or equipment.
- The Contractor shall ensure that all personnel assigned to this contract understand and adhere to the Privacy Act of 1974.
- Contractors shall comply with all Government security procedures and ensure security measures are in place to protect equipment and data from physical and virus damage, theft, loss, or access by unauthorized individuals. (See AFMAN 17-1203, AFI 33-138, *Incident Response and Reporting*, AFI 33-200, *Information Assurance (IA) Management*, AFMAN 33-223, *Identification and Authentication*, Air Force Systems Security Instruction (AFSSI) 8502, *Organizational Computer Security*, AFSSI 8522, *Access to Information Systems*, and AFSSI 8580, *Remanence Security*).
- Contractor personnel shall complete mandated training required for performance of this contract in accordance with AFI 36-2201, *Air Force Training Program*, paragraph 7.4.10., as stated below and/or as required by the AFRC/A6 COR. The required training shall be completed prior to commencing performance with evidence of course completion submitted to the COR:
  - DoD Information Assurance Awareness (ZZ133098)
  - Security Administration (ZZ133078)
  - Fire Extinguisher Safety (AFI 91-203)
  - For personnel with classified IS access, the following training is required IAW AFI 16-1404, *Air Force Information Security Program*:
    - Derivative Classification (every 2 years)
    - Marking Course (1 time requirement)
- Training Certificates. The contractor personnel shall provide certificates of required Government training.

4.18.2. Data Integrity. Data pertaining to other contracts and services reside on systems used by AFRC. The Contractor shall not divulge this information or use this information for the contractor's gain. In addition, any and all records, files, documents, and work papers, regardless of the type of media created in (e.g., physical, electronic, etc.) provided

and/or generated by the Government and/or generated for the Government in performance of this PWS, maintained by the Contractor which are to be transferred or released to the Government or successor Contractor, shall become and remain Government property and shall be maintained and disposed of IAW AFMAN 33-363, *Management of Records*; AFI 33-364, *Records Disposition – Procedures and Responsibilities*; the Federal Acquisition Regulation, and/or the Defense Federal Acquisition Regulation Supplement, as applicable.

4.18.3. Safeguarding Classified Information**:**

4.18.3.1. The Contractor shall comply with all security regulations and directives as identified herein and other security requirements as are shown elsewhere in this contract. The Contractor shall comply with DD Form 254, **DoD Contract Security Classification**, attached to this contract.

4.18.3.2. The Contractor shall conform to the provisions of *DOD 5220.22M, National Industrial Security Program Operating Manual (NISPOM),* DoD 5220.22-R, *Department of Defense Industrial Security Program*, DoDM 5200.1, Volumes 1-4, AFI 16-1404, and AFI 16-1406, *Air Force Industrial Security Program*.

4.18.4 Industrial Security. (Include this subject if DD 254 is required)

4.18.4.1 DD Form 254. The Contractor shall comply with the DD254, *DoD Contract Security Classification*, attached to Section J of this contract. Contract performance is restricted to the Federal installations and government facilities identified by the government in the DD 254.

4.18.4.2 Visitor Group Security Agreement (VGSA). The Contractor shall enter into a visitor group security agreement at the time of contract award with each installation. The Contractor shall comply with AFFARS 5352.204-9000, *Notification of Government Security Activity and Visitor Group Security Agreements* (March 2012). There will be no contract performance until the VGSA is signed at each installation. VGSAs must be signed during phase in period.

4.18.4.3 Facility Clearance. The Contractor shall comply with AFFARS 5352.215-9000, *Facility Clearance* (MAY 1996) in Section H of this contract.

4.18.4.4. Foreign Ownership, Control & Influence. The Contractor will comply with paragraphs 2-303C(2) of the National Industrial Security Program Operating Manual (NISPOM), 28 February 2006, to include Change 1, 28 March 2013, and Enclosure 3, Paragraph 3a of DoDM 5220.22-V3, *National Industrial Security Program: Procedures for Government Activities Relating to FOCI*, 17 April 2014, AFI 16-1406, *Air Force Industrial Security Program*, 25 August 2015, ODAN 17-12, and DTM 15-002, *Policy Guidance for the Processing of an NID in Connection with FOCI*, 25 February 2016 contain clarifications to policy regarding NIDs.

4.18.5. Personnel Security:

4.18.5.1. Background Investigations. As a minimum, all Contractor personnel must have a SECRET clearance. The following items also apply:

- A National Agency Check with Local Agency Check and Credit Check (NACLS) Clearance is required.
- NACI for unclassified network access and CAC issuance.
- All personnel shall have an **interim SECRET** prior to employment.
- Certification Authority Workstation (CAW) requires a FINAL Secret prior to starting work.
- If a person is declined an appropriate clearance then they must be removed from the contract.
- After Designated Approval Authority (DAA) approval for connectivity to an Air Force network, the network administrators, system administrators, and organization computer managers will restrict access to the minimum necessary to fulfill defined mission requirements.

4.18.5.2. The Contractor shall obtain personnel security clearances on all employees who require unescorted entry into open storage areas, access to classified material, use of unclassified automated and classified information systems that have access to sensitive information (IT/AIS Level II), and access to the base network within 15 calendar days after receipt of the facility clearance or 60 days prior to performance start date if the contractor possesses a facility clearance.

4.18.5.3. Every AF network user must possess a current and favorable National Agency Check with Written Inquires (NACLC) Investigation.

4.18.6. Facility Clearances and Employee Clearance. The Contractor shall possess or obtain a facility clearance at the classification level of SECRET.

4.18.6.1. The Personnel Security Section (Installation IP Office) will process and forward requests for Contractor NACIs for suitability determinations. The Contractor is responsible for processing NACLCs.

4.18.6.2. Upon completion of the subsequent investigation suitability of employment review, (Installation IP Office) will notify the unit Commander (or designee) of the organization for employee receiving a favorable/unfavorable NACI. The Contracting Officer will notify the Contractor of employees receiving a favorable/unfavorable NACI by forwarding a copy of the Record of Employment Suitability Form to the Contractor. The Contractor's employee(s) will not be allowed access to sensitive information or restricted areas when the current NACI is unfavorable.

4.18.6.3. When the Government is in the process of conducting a NACI investigation on a Contractor employee and that individual's employment is terminated before the investigation is completed, the Contractor shall immediately forward to (Installation IP Office) written notice of the termination.

4.18.6.4. Pending favorable NACI, contractor employees shall be escorted at all times.

4.19. **Contractor Identification.** The Contractor personnel shall wear contractor-provided identification at all times while in government facilities so as to distinguish themselves from Government employees. Contractor personnel may attend meetings, answer phones, and work in other situations where their status is not obvious to third parties; therefore, the Contractor personnel shall always identify themselves as Contractor support to avoid potential misrepresentation as Government personnel or to avoid situations arising where sensitive topics might be better discussed solely amongst government personnel. Electronic mail signature blocks shall identify their company affiliation. Where practicable, Contractor personnel occupying collocated space with their Government program customer shall identify their work space with their name and company affiliation.

4.20. **Network Security:**

4.20.1. Network access is a privilege extended to contractor employees. It will be granted only after all criteria have been met and may be suspended for cause as defined in AFI 33-115V2, Section 5.6. Network access will be approved IAW AFI 31-501, *Personnel Security Program Management;* AFI 16-1406; AFI 33-115V1, *Network Operations (Netops)*; AFI 33-115V2, *Licensing Network Users and Certifying Network Professionals,* AFI 33-202, AFMAN 33-223, *Identification and Authentication*; DoD 8510.01, *DoD Information Assurance Certification and Accreditation Process (DIACAP),* and DoD 5220.22-M, *National Industrial Security Program Operating Manual (NISPOM).* Per AFI 33-115V2, "every individual who has access to the Air Force network (af.mil) domain, specialized systems and mission systems is a network user. Before becoming an AF network user, an individual must be trained and licensed. This process of training and licensing ensures that every Air Force network user is trained and aware of the basic principles of network security and their role in Information Assurance (IA)."

4.20.2. No Foreign Nationals will be used for this contract.

4.21. **Physical Security:**

4.21.1. Installation Perimeter Access Control. The requirements for installation perimeter access are detailed in Air Force Federal Acquisition Regulation Supplement (AFFARS) clause 5352.242-9000 entitled, *Contractor Access to Air Force Installations,* in Section I, *Contract Clauses,* of the basic contract.

4.21.1.1. The Contractor shall obtain base identification, if required, for all Contractor personnel who make frequent visits to or perform work on the Air Force installation(s) cited in the contract. Contractor personnel are required to wear or prominently display installation identification badges or contractor-furnished, contractor identification badges while visiting or performing work on the installation.

4.21.1.2. During performance of the contract, the Contractor shall be responsible for obtaining required identification for newly assigned personnel and for prompt return of credentials for any employee who no longer requires access to the work site.

4.21.1.3. Upon completion or termination of the contract or expiration of the identification passes, the prime Contractor shall ensure that all base identification passes issued to employees and subcontractor employees are returned to the issuing office.

4.21.1.4. Failure to comply with these requirements may result in withholding of final payment.

4.21.2. Resource Protection and Integrated Defense. The Contractor shall safeguard all Government property in accordance with AFI 31-101, *Integrated Defense*, and any forms provided for Contractor use. The Contractor shall immediately report all thefts, vandalism, or destruction of property and equipment (Government or Contractor owned) to the AFRC/A6 Directorate Security Manager or Alternate Security Manager and COR.

4.21.3. USAF Restricted Area and Controlled Area Access. The requirements for USAF Restricted Area and Controlled Area access are detailed in AFI 31-101, *Integrated Defense*, and governed at each installation by the Integrated Defense Plan.

4.21.4. HQ AFRC Facility Access. The Contractor personnel shall be issued access control badges which will allow access to work centers, as applicable.

4.21.5. Information Security:

4.21.5.1. Controlled Unclassified Information Security**.** The Contractor shall handle and safeguard Controlled Unclassified Information in accordance with DoD Manual 5200.1-M, Volume 4 entitled, *DoD Information Security Program: Controlled Unclassified Information (CUI)*.

4.21.5.2. Information Protection Program. The Contractor shall participate in the host installation's Information Protection Program (IPP).

4.21.5.3. Privacy Act (PA). The Contractor personnel shall have access to Privacy Act information that requires adherence with the Privacy Act of 1974, Title 5 of the U.S. Code, Section 552a, AFI 33-332, *Air Force Privacy Act Program*, and other applicable agency rules and regulations. The Contractor personnel shall follow agency procedures to identify and safeguard reports and data accordingly. The Contractor shall ensure that

Contractor personnel assigned to this requirement are briefed annually on properly identifying and handling Privacy Act data and reports.

4.21.6. General Common Access Cards (CACs) Information:

4.21.6.1. For installation(s)/location(s) cited in the contract, Contractors shall ensure Common Access Cards (CACs) are obtained by all contract or subcontract personnel who meet one or both of the following criteria:

4.21.6.1.1. Require logical access to DoD computer networks and systems in either:

4.21.6.1.2. The unclassified environment; or

4.21.6.1.3. The classified environment where authorized by governing security directives.

4.21.6.2. Perform work which requires the use of a CAC for installation entry control or physical access to facilities and buildings.

4.21.6.3. Contractors and their personnel shall use the following procedures to obtain CACs:

4.21.6.4. While visiting or performing work on installation(s)/location(s), Contractor personnel shall wear or prominently display the CAC as required by the governing local policy.

4.21.6.5. During the performance period of the contract, the Contractor shall:

4.21.6.6. Return CACs in accordance with local policy/directives within 7 working days of a change in status for Contractor personnel who no longer require logical or physical access.

4.21.6.7. Report lost or stolen CACs in accordance with local policy/directives.

4.21.6.8. Within 7 working days following completion/termination of the contract, the Contractor shall return all CACs issued to their personnel to the issuing office or the location specified by local policy/directives.

4.21.6.9. Failure to comply with these requirements may result in withholding of final payment.

4.21.7. Specific Instruction for AFRC CAC Processing. Common Access Card (CAC) Issue Procedures. Every Contractor, regardless of which location they work at, will be required to have a CAC in order to access the network. With that said, the procedures for the issuance of CACs will be as follows:

4.21.7.1. The Vendor Program Manager will verify the individual has a security clearance.

4.21.7.2. Once verified, the Vendor Program Manager will complete the Trusted Agent Authorization to Issue Common Access Card (CAC).

4.21.7.3. The completed form will either be hand-carried over to the COR or scanned and sent via email to the COR in .pdf format. NOTE: The letter shall be legible to the COR; anything considered not legible, will be returned back to the vendor for correction and resubmittal.

4.21.7.4. The COR will sign the letter and input the information into the Trusted Associate Sponsorship System (TASS) database.

4.21.7.5. Once inputted into the TASS database, the COR will notify the individual (Contractor requiring the CAC) by email. Once notified, the Contractor will have 7 days to access the website and provide the information required. If not accomplished within 7 business days, the request will automatically be deleted from the TASS database and the Contractor will have to start the process over (See para 4.18.13.).

4.21.7.6. Once the Contractor has completed all requirements, then the COR will be notified via email to go into the TASS database and approve the CAC application. Once the COR approves the CAC request, the Contractor will be notified via email that the CAC application was approved and then will be allowed to report to the nearest Military Personnel Flight (with 2 pieces of ID) to get issued their CAC.

4.22. Standards and References. Hardware and software manuals for systems supported under this contract will be made available and shall remain property of the Government.

4.23. Contractor Manpower Reporting (via eCMRA). In accordance with the Office of the Secretary of Defense (OSD) Memorandum, Enterprise-wide Contractor Manpower Reporting Application, dated 28 Nov 2012, the Contractor shall report all Contractor labor hours, including subcontractor labor hours, required for performance of the services provided under the contract at the Enterprise-wide Contract Manpower Reporting Application (eCMRA) site below. Reporting shall be conducted for each fiscal year (FY), which extends 01 October through 30 September. While inputs may be made any time during the FY, all data shall be reported no later than 31 October of the following FY. The Contractor may direct questions to the help desk at the eCMRA site below http://www.ecmra.mil.

4.24. Uses and Safeguarding of Information. Information from the secure web site is considered to be proprietary in nature when the contract number and contractor identity are associated with the direct labor hours and direct labor dollars. At no time will any

data be released to the public with the contractor name and contract number associated with the data.

4.25. User Manuals. Data for Air Force service requirements must be input at the Air Force CMRA link. User manuals for Government personnel and contractors are available at the Army CMRA link at http://www.ecmra.mil.

4.26. **Designation of Services as Mission-Essential.** In accordance with DFARS 237.7602(a), *The Continuation of Essential Contractor Services/Policy*, DFARS 252.237-7023(a)(2), and AFI 10-403, *Deployment Planning and Execution*, paragraph 1.9.1.33.2, the Functional Commander (FC) or civilian equivalent has determined these services are **not mission-essential** and will not continue in the event of a crisis.

4.27. Services Delivery Summary. The Services Summary addresses elements of the Government's quality assurance program. The Government will review the Contractor's performance under this contract as specified in the Quality Assurance Surveillance Plan (QASP). The QASP provides a structure for Government surveillance of the Contractor's performance to ensure it meets the performance standards set forth below. Surveillance methods may include periodic surveillance of the Contractor's performance, periodic reports and briefings provided to all levels of leadership. The QASP establishes roles and responsibilities of the Multi-Functional Team (MFT), procedures for assessment/inspection, and process for continuous oversight. The Contractor is responsible for providing and implementing performance that meets, at a minimum, the performance standards set forth below using its Quality Control Plan.

4.27.1. Quality Control Plan (QCP):

4.27.1.1. In compliance with standards as specified in the requirements per Section 2 and 3 of this document, the contractor shall provide and maintain a Quality Control Plan (QCP) that contains, as a minimum, the items listed in 4.27.2. to the CO for acceptance not later than (NLT) five (5) work days after the start of this contract. The CO will notify the contractor of acceptance or required modifications to the plan within five (5) work days. The contractor shall make appropriate modifications and obtain final acceptance of the plan by the CO within five (5) work days of notification of required changes.

4.27.1.2. The plan shall include the following minimum requirements:

- A description of the inspection system to cover all services listed in the Performance Standards (see para 4.27.2.). Description shall include specifics as to the areas to be inspected on both a scheduled and unscheduled basis, frequency of inspections, and the title and organizational placement of the inspectors. Additionally, control procedures for any Government provided keys or lock combination should be included.
- A description of the methods to be used for identifying and preventing defects in the quality of service performed.

- A description of the records to be kept to document inspections and corrective or preventive actions taken.
- All records of inspections performed shall be retained and made available to the Government upon request throughout the contract period of performance, and for the period after contract completion, until final settlement of any claims under this contract.

4.27.2. Performance Standards. The following table identifies the performance standards that will be measured by the Government, as a minimum. The Contractor shall have these elements as part of their Quality Control Program and may have others, as necessary, to meet Contractor quality standards. The Contractor shall ultimately be responsible for all tasks and deliverables identified in this PWS.

NOTE: The Contractor shall be responsible for compliance to individual project schedule milestones as jointly agreed between the Government and Contract Program Manager. The Government will develop and deliver a list of key projects to the Contractor. The Contract Program Manager will deliver to the Government elements of the Monthly Key Project Status (MKPS) Report as defined in 2.1.1. Key projects are subject to change at the discretion of the Government.

Services Summary:

Performance Objective (defines the desired outcomes)	**PWS Para Ref**	**Performance Threshold (defines the level of service required to successfully meet the objective)**	**Surveillance Method (defines how, who, when, what will be used to measure performance)**
Meet individual project schedule milestones for key projects designated by the Government	2., 3.	Meet project schedule milestones on-time delivery at 90% level	100% Inspection of monthly MKPS report
Provide accurate/comprehensive MTS, MFS, MPS, MKPS, and Monthly Metrics reports within 10 work days after end of month	2.1.1.	On-time delivery at 100% level	100% Inspection of MTS/MFS/MPS/MKPS, and Monthly Metrics reports
Ensure that the contractor maintains an acceptable manning rate	2.1.1., 4.4.	Maintain contractor manning at ≥90% of the proposal	100% Inspection of Monthly Metrics Report

Performance Objective (defines the desired outcomes)	PWS Para Ref	Performance Threshold (defines the level of service required to successfully meet the objective)	Surveillance Method (defines how, who, when, what will be used to measure performance)
Ensure that the contractor maintains an acceptable monthly lapse rate	2.1.1., 4.4.	Maintain monthly average lapse rate of ≤15 calendar days	100% Inspection of Monthly Metrics Report
Provide monthly VTC usage report detailing number of calls, bridging method (e.g., point-to-point, GVS or HQ VTC Bridge) and success rate (e.g., average packet loss during session, if the session disconnected or dropped, etc)	2.1.1., 2.6.1., 3.8.1.1., 3.8.3.1.	99% success rate of VTC sessions per month	100% inspection of monthly MTS usage reports
Provide accurate/comprehensive project portfolios	2.2.4.	Projects will have a portfolio established within 30 days of assignment; reviewed weekly to incorporate changes	Periodic inspection
Deliver Annual Operating Plan and IMS within 60 days of receipt of Government EA Program Plan; with quarterly updates due the 1st work day of each quarter thereafter	2.9.1.1., 2.9.1.4.	On-time delivery at 100%	100% inspection
Meets scheduled milestones identified in Annual Operating Plan and IMS, as approved by Government	2.9.1.1.	On-time delivery at 95%	100% inspection
Ensure NIPR/SIPR CAT vulnerabilities for each assigned server does not exceed AFRC, AF, DISA, or DoD vulnerability thresholds	3.4., 3.5., 3.6., 3.7., 3.8.	Must be ≤2.49 vulnerabilities per each assigned server	100% inspection of monthly Gov't scans; 100% inspection of data reported in metrics

Performance Objective (defines the desired outcomes)	PWS Para Ref	Performance Threshold (defines the level of service required to successfully meet the objective)	Surveillance Method (defines how, who, when, what will be used to measure performance)
Server administrators will implement AF Maintenance Tasking Orders (MTOs), TCNOs, and CCOs by established deadlines	3.4., 3.5., 3.6., 3.7., 3.8.	100% compliance for MTOs; 95% compliance for TCNOs	100% inspection of monthly reports
HQ AFRC only: CSC will ensure NIPR/SIPR CAT vulnerabilities for each workstation does not exceed AFRC, AF, DISA, or DoD vulnerability thresholds	3.7.2.	Must be <2.49 vulnerabilities per workstation	100% inspection of monthly Gov't scans; 100% inspection of data reported in metrics
HQ AFRC only: CSC will maintain customer satisfaction levels specified	3.7.2.	85% Customer Satisfaction	Quarterly review of survey results
HQ AFRC only: Provide Client Support Centers (CSCs) Support	3.7.2.	By the first business day of the week, ≤50 unresolved tickets in the queue for the previous week and <85% of all tickets that were closed during the week were not open longer than 14 days	100% Inspection of Remedy Reports
Provides configuration control documentation of system changes	3.8.4.2.4	On-time delivery at 100% level (Monthly)	100% Inspection of all reports
Minimizes services, application, and system unscheduled downtime	3.4.12., 3.8.4., 3.8.5.	99% availability for the month with no more than 7 hours of downtime within contractor's control	Periodic Inspection

4.28. Quality Assurance. The Government will evaluate the contractor's performance of this contract. For those services listed in the Performance Standards, the COR, or evaluators will follow the method of surveillance specified in this contract. Government personnel will record all surveillance observations. When an observation indicates defective performance, the COR, or evaluators will require the contract manager or representative at the site to initial the observation. The initialing of the observation acknowledges that he or she has been made aware of the defective performance and does not necessarily constitute concurrence with the observation. Government surveillance of services not listed in the Performance/ Deliverables Matrix or by methods other than those listed in the Performance/Deliverables Matrix (such as provided in the Inspection of Services clause) may occur during the performance period of this contract. Such surveillance will be done according to standard inspection procedures or other contract provisions. Any action taken by the CO as a result of surveillance will be according to the terms of this contract.

4.29. Contractor Performance Assessment Reporting System (CPARS)/Past Performance. The Government will provide and record past performance Information for acquisitions over $150,000 utilizing the Contractor Performance Assessment Reporting System (CPARS). The CPARS process allows contractors to view and comment on the Government's evaluation of the contractor's performance before it is finalized. Once the contractor's past performance evaluation is finalized in CPARS it will be transmitted into the Past Performance Information Retrieval System (PPIRS).

Contractors are required to register in the CPARS, in order to review and comment on past performance reports submitted through the CPARS.

CPARS: **https://www.cpars.csd.disa.mil/ or https://www.cpars.gov**
PPIRS: **http://www.ppirs.gov**

4.30. Personal Services:

Administration and monitoring of the contractor's performance by GSA CO, Program Manager, and the COR shall not be as detailed or continual as to constitute supervision of contractor personnel. Government personnel may not perform any supervisory functions for contractor personnel, such as interviewing, appraising individual performance, scheduling leave or work, or directing how to perform work.

To counter the circumstances that infer personal services and to preserve the non-personal nature of the contract, the contractor shall adhere to the following guidelines in the performance of the task:

- Provides for direct supervision of all contract employees assigned to the task.

- Refrains from discussing the issues such as skill levels and hours, salaries, cost and funding data, or administrative and personnel matters affecting contractor employees.
- Ensures close communication/coordination with the COR, reporting problems as they occur (not waiting for a monthly meeting).
- Does not permit Government officials to interview potential contractor employees, discuss individual performance, approve leave or work scheduling of contractor employees, terminate contractor employees, assist contractor employees in doing their jobs or obtain assistance from the contractor in doing Government jobs.
- Does not assign contractor personnel to work under direct Government supervision.
- Maintains a professional distance from Government employees.
- Provides contractor employees with badges, if appropriate, identifying them as contractors.
- Ensures proper communications with the Government. Technical discussion and Government surveillance is acceptable, but the Government cannot tell the contractor how to do the job.
- Assigns a task leader to the contract. The task leader or alternate should be the only one who accepts tasking from the assigned Government point of contact or alternative.
- Uses work orders to document and manage the work and to define the details of the assignment and its deliverables. The Government has the right to reject the finished product or result and this does not constitute personal services.
- When travel is required for the performance on this contract, contractor personnel are only to travel as directed by their contract management.

4.31. Compliance Documents. The Contractor shall comply with the latest edition of the following directives, instructions, regulations, manuals and statutes. (See Table 2 for a list of all publications and forms.)

4.32. Compliance with Section 508 (if applicable). All electronic and information technology (EIT) procured through this contract must meet the applicable accessibility standards at 36 Code of Federal Regulations (CFR) 1194, unless an agency exception to this requirement exists; 36 CFR 1194 implements Section 508 of the Rehabilitation Act of 1973, as amended, and is viewable at http://www.accessboard.gov/sec508/508standards.htm. The contractor shall indicate for each line item in the schedule whether each product or service is compliant or noncompliant with the accessibility standards at 36 CFR 1194. Further, the proposal must indicate where full details of compliance can be found (e.g., vendor's website or other specific location).

4.33. Definitions. The following definitions and descriptions apply:

- "**Government On-Site Lead [also known as the Quality Assurance (QA) at a particular base]"** is the inherently Governmental Quality Assurance Representative at each location who is responsible for ensuring the contractor is performing all said duties at the particular location (base). This is normally the CS/CF commander and/or his/her Senior ART.
- "**Contractor**" includes the prime contractor, parent company, affiliates, divisions, and subsidiaries.
- "**Contracting Officer**" is the GSA appointed representative who has the overall responsibility for the management of this contract. The CO is the only person authorized to make changes to the terms and conditions of the contract.
- "**Contracting Officer Representative (COR)"** is the individual is responsible for looking out for the best interests of the Government in regards to this contract.
- "**Contractor Site Lead**" is the individual contractor who has the overall responsibility for the day-to-day management of this contract at their particular site (base). This individual makes all on-site decisions in regards to the management of this contract.
- "**Development**" includes all efforts toward solution of broadly defined problems. This may encompass research, evaluating technical feasibility, proof of design and test, or engineering of programs not yet approved for acquisition or operation.
- "**On-Site Program Manager**" is the individual contractor who has the overall responsibility for the day-to-day management of this contract. This individual will be the one assigned locally (to the Robins AFB, GA vicinity) that makes all the on-site decisions in regards to this contract.
- "**Program Manager (PM)"** is the individual is responsible for the management of this contract as well as looks out for the best interests of the Government in regards to this contract.
- "**Proprietary Information**" includes all information designated as proprietary IAW applicable laws and regulations, and held in confidence or disclosed under restriction to prevent uncontrolled distribution. Examples include limited or restricted rights data, trade secrets, sensitive financial information, and computer software. Proprietary information may appear in technical data, cost and pricing data, or may involve classified information. For the purpose of this definition, proprietary information pertains to both contractor and Government information, regardless of format.

4.34. Safety:

4.34.1. Health & Safety Program. The Contractor is responsible for the safety and health of their personnel and protection of the public on Government work sites (DODI 6055.1, Paragraph E5.1). The Contractor shall maintain a health and safety program that meets Occupational Safety and Health Administration (OSHA) standards. If the CO notifies the Contractor of a potential OSHA violation, the Contractor is obligated to comply with the

applicable OSHA regulations. If the Government identifies that additional safety equipment is required (e.g., steeltoe boots, etc.…), it shall be the Contractor's responsibility to procure these items for their applicable contractors.

4.34.2. Incident or Mishap Procedures. The contractor shall immediately call 911. The Contractor shall within one (1) hour notify the COR/CO and Government Safety Manager of all mishaps or incidents at or exceeding $2,000 (material + labor) for damage to Government property. This notification requirement shall also include physiological mishaps/incidents. A written or email copy of the mishap/incident notification shall be sent within three (3) calendar days to the COR who will forward to the Government Safety Manager. For information not available at the time of initial notification, the Contractor shall provide the remaining information not later than twenty (20) calendar days after the mishap, unless extended by the COR/CO. Mishap notifications shall contain, as a minimum, the following information:

- Contract, contract number, name and title of person(s) reporting
- Date, time and exact location of accident/incident
- Brief narrative of accident/incident (events leading up to the accident/incident)
- Cause of accident/incident (if known)
- Estimated cost of accident/incident (material + labor to repair/replace)
- Nomenclature of equipment and personnel involved in the accident/incident
- Corrective actions (taken or proposed)
- Other pertinent information

The Contractor shall, in the event of an accidental incident/mishap, take reasonable action to establish control of the incident/mishap scene, prevent further damage to persons or property, and preserve evidence until released by the incident/mishap investigative authority.

4.34.3. Fire Emergencies. The Contractor personnel shall dial 911 to report fire related emergencies.

4.34.4. Department of Labor Inspection of Contractor Operations. The Contractor is subject to Department of Labor (DoL) inspections and enforcement by OSHA health and safety officials while performing work on a Government installation. The OSHA health and safety officials may access workplaces on Government installations at any time, scheduled or unscheduled, during regular work hours. The OSHA health and safety officials must meet security requirements to enter restricted or classified areas. The Contractor shall notify the COR/CO upon notification of a visit.

4.34.5. Fire Prevention Training. The contractor personnel who work on a Government installation shall participate in fire extinguisher training in accordance with AFI 91-203, paragraphs 6.2.1, 6.2.16 and 6.2.17.

4.34.6. Fire Protection and Prevention Program. All contractor personnel performing work on properties under jurisdiction of the Government shall be responsible for fire safety and compliance with all applicable OSHA, State, Air Force, AFRC, and base regulations and directives. The contractor personnel shall attend a contractor's briefing on fire safety prior to any work. The contractor shall ensure that all contractor personnel and sub-contractors under their control are briefed on fire prevention practices in accordance with applicable directives. The contractor personnel who work on Robins AFB, GA are required to take annual fire prevention refresher training in accordance with RAFBI 32-2001, paragraph 2.4. NOTE: This applies to Robins AFB, GA; all other installations will follow their applicable local directives.

4.35. Environmental Management System (EMS).

4.35.1. Executive Order (E.O.) 13423, *Strengthening Federal Environmental, Energy, and Transportation Management*, and E.O. 13514, *Federal Leadership in Environment, Energy, and Economic Performance*, establish the requirement for an EMS.

4.34.2. In accordance with the Assistant Secretary of the Air Force (SAF) Policy Letter, *Conformance with Air Force Environmental Management System (EMS) Requirements for Contracts Performed on Air Force Installations*, dated 11 Dec 06, Contractor personnel who perform work on any USAF installation shall comply with the EMS requirements established by the installation.

4.34.3. Contractor personnel shall complete EMS training prior to beginning work on any USAF installation.

The EMS training requirement may be satisfied by any of the following means:

1) If the Contractor is International Organization for Standardization (ISO) 14000 (Environmental management) certified, Contractor personnel do not have to complete EMS training; however, the Contractor must provide documentation of ISO 14000 certification to the PCO.

2) If Contractor personnel possess CACs, they may complete EMS - General Awareness Training at the Advanced Distributed Learning Service (ADLS) site below. The Contractor shall provide their certificate(s) to the PCO. https://golearn.csd.disa.mil/kc/login/login.asp?kc_ident=kc0001

4.34.4. The prime Contractor shall ensure subcontractors comply with the EMS requirement.

4.35. Invoicing/Payment and Receipt/Acceptance:

The invoice must be submitted to GSA ASSIST and the Central Invoice System (CIS) web-based Order Processing System (https://portal.fas.gsa.gov/). The Client

Representative (COR) and the GSA Customer Account Manager or Contract Specialist must approve the invoice in CIS prior to payment.

4.35.1 The payment information must satisfy a match between CIS and SAM for the invoice to be successfully processed for payment.

4.35.2 If the contractor submits a revised invoice, the revised invoice must include: 1) a unique invoice number, 2) a brief explanation, and 3) a cross-reference to any previous invoice submittals for tracking purposes and avoiding duplication.

4.35.3 Receipts, travel vouchers, etc. to support charges for other than employee labor hours must be completed in accordance with applicable Government regulations. The contractor shall maintain originals and make them available to the Government upon request. The contractor will also provide copies when requested by the Government.

4.35.4 Reimbursable costs must not exceed the limit(s) specified in the task order. The Government will not pay charges that are not specifically identified in the task and approved, in advance, by the Government.

4.35.5 Invoices for final payment must be so identified and submitted when the task has been completed and no further charges are to be billed.

4.36. Inspection of Services:

4.36.1. In accordance with *FAR 52.246-4, Inspection of Services - Fixed-Price; and FAR 52.246-6, Inspection - Time-and-Material and Labor-Hour,* the Government reserves the right to inspect Contractor performance.

4.36.2. In accordance with *FAR 52.246-4, Inspection of Services - Fixed-Price; and FAR 52.246-6, Inspection - Time-and-Material and Labor-Hour,* the Contractor shall maintain an inspection process acceptable to the Government. The Contractor and shall maintain records of inspections which shall be made available to the Government as long as the contract requires.

4.37. Government Points of Contact:

4.37.1. Contracting Officer Representatives. The Contracting Officer will designate a COR in accordance with DFARS 252.201-7000 for this contract. The COR provides the Contractor personnel access to all available Government-furnished information, facilities, material, equipment, services, etc. as required, for this requirement. The COR also provides assistance to the AFRC/PKA CO with technical monitoring of the requirement and administration of the contract.

4.37.2. Points of Contact. A list of the Government team members for contract surveillance including the Contracting Officer and Contracting Officer Representative with applicable contact information is included in the COR Designation memorandum.

TABLE 1
ACRONYMS AND ABBREVIATIONS

1B1N	One Base One Network
24/7	24 hours-a-day/7 days a week
24 AF	24th Air Force
38 EIG	38th Engineering Installation Group
301 FW	301st Fighter Wing (NAS-JRB Ft Worth, TX)
304 RS	304st Rescue Squadron (Portland IAP, OR)
434 ARW	434th Air Refueling Wing (Grissom ARB, IN)
439 AW	439th Airlift Wing (Westover ARB, MA)
452 AW	452nd Airlift Wing (March ARB, CA)
482 FW	482nd Fighter Wing (Homestead ARB, FL)
910 AW	910th Airlift Wing (Youngstown ARB, OH)
911 AW	911th Airlift Wing (Pittsburgh ARS, PA)
919 CS	919th Communications Squadron (Duke Field, FL)
AC	Air Conditioning
ACAS	Assured Compliance Assessment Solution
ACO	Acquisition Accounting Officer
ACP	Allied Communications Publication
AD	Active Directory
ADLS	Advanced Distributed Learning Service
AF	Air Force
AFB	Air Force Base
AFCAP	Air Force Certification and Accreditation Program
AFDCCI	Air Force Datacenter Consolidation Initiative
AFDS	Air Force Directory Services
AFFARS	Air Force Federal Acquisition Regulation Supplement
AFI	Air Force Instruction
AFMAN	Air Force Manual
AFNet	Air Force Network
AFRC	Air Force Reserve Command
AFSMO	Air Force Spectrum Management Office
AFSPC	Air Force Space Command
AFSSI	Air Force Systems Security Instruction
AIM	Asset Inventory Management
AN	Access Nodes
ANSI	American National Standards Institute
AO	Accountable Officer

AoA	Analysis of Alternatives
APL	Approved Product List
ARB	Air Reserve Base
AROWS-R	Air Force Reserve Orders Writing System-Reserve
ARS	Air Reserve Station
ASNTs	Aircrew Strategic Network Terminals
ATO	Authority to Operate
A/V	Audio/Visual
AV	All View
AW	Airlift Wing
BAN	Base Area Network
BDC	Business Data Connectivity
BEA	Business Enterprise Architecture
BER	Beyond Economic Repairs
BI	Business Intelligence
BITI	Base Information Transport Infrastructure
BRM	Business Reference Model
C2	Command and Control
C&A	Certification and Accreditation
C&I	Communications and Information
CAC	Common Access Card
CAN	Critical Access Nodes
CAS	Client Access Server
CAW	Certification Authority Workstation
CCI	Controlled Cryptographic Items
CCNA	Cisco Certified Network Associate
CCRI	Cyber Command Readiness Inspection
CDN	Critical Distribution Nodes
CDRL	Contract Data Requirement Listing
CEA	Chief Enterprise Architect
CFR	Code of Federal Regulations
CFP	Communication Focal Point
CIO	Chief Information Officer
CITS	Combat Information Transport System
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CJCSM	Chairman of the Joint Chiefs of Staff Manual
CLIN	Customer Line Item Number
CN	Core Nodes
CND	Computer Network Defense
CO	Contracting Officer
COA	Course of action
COI	Community of Interest
COMPUSEC	Computer Security

COMSEC	Communications Security
CONOPs	Concept of Operations
CONUS	Continental United States
COOP	Continuity of Operations
COR	Contracting Office Representative
CORT	Contracting Officer's Representative Tracking
COTS	Commercial off-the-Shelf
CPARS	Contractor Performance Assessment Reporting System
CRM	Customer Relationship Management
CST	Client Support Technician
CTI	Computer Telephony Integration
DAA	Designated Approval Authority
DBA	Database Administrator
DCID	Director of Central Intelligence Directive
DCORs	Datacenter Obligation Requests
DD	Department of Defense
DFARS	Defense Federal Acquisition Regulation Supplement
DHCP	Dynamic Host Configuration Protocol
DIACAP	DoD Information Assurance Certification and Accreditation Process
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DMM	Domestic Mail Manual
DMS	Defense Messaging System
DN	Distribution Nodes
DNI	Department of National Intelligence
DNS	Domain Name Service
DoD	Department of Defense
DoDAF	Department of Defense Architecture Framework
DODD	Department of Defense Directive
DODI	Department of Defense Instruction
DODM	Department of Defense Manual
DOL	Department of Labor
DSE	Dedicated Support Engineer (DSE)
DSN	Defense Switched Network
DT	Development Team
EA	Enterprise Architecture
EC	Equipment Custodian
ECO	Equipment Control Officer
EIA	Electronic Industries Association
EIT	Electronic and Information Technology
EL-CID	Equipment Location-Certification Information Database
E-mail	Electronic Mail

EMC	Egan Marino Corporation
EMS	Environmental Management System
ENFAAS	Enclave NIPR Firewall and ASIM Sustainment
EO	Executive Order
ESB	Enterprise Service Bus
ESD	Enterprise Service Desk
ESU	Enterprise Service Unit
ETL	Extract Translate and Load
FAA	Federal Aviation Administration
FAR	Federal Acquisition Regulation
FC	Functional Commander
FCC	Federal Communications Commission
FDCC	Federal Desktop Core Configuration
FDO	Foreign Disclosure Office
FFP	Firm Fixed Price
FIPS	Federal Information Processing Standard
FM	Financial Management
FOIA	Freedom of Information Act
FOUO	For Official Use Only
FRRS	Frequency Resource Record System
FSO	Functional Security Officer
FTE	Full-time Equivalent
FTP	File Transfer Protocol
FY	Fiscal Year
GAL	Global Address List
GCCS	Global Command and Control System
GFE	Government Furnished Equipment
GIG	Global Information Grid
GILS	Government Information Locator Service
GMF	Government Master File
GSA	General Service Administration
HP	Hewlett Packard
HQ	Headquarters
HQ USAF/RE	Headquarters United States Air Force, Office of Reserve Affairs
HQ AFRC	Headquarters Air Force Reserve Command
HQ AFRC/A6	Headquarters Air Force Reserve Command Director of Communications
HQ AFRC/A6OD	Headquarters Air Force Reserve Command Director of Communications Force Management Branch
HQ AFRC/SCOS	Headquarters Air Force Reserve Command Director of Communications Networks Division

HQ AFRC/A6XC	Headquarters Air Force Reserve Command Director of Communications Chief Information Officer (CIO) Support Branch
HQ AFRC/A6XP	Headquarters Air Force Reserve Command Director of Communications Plans and Program Branch
HQ AFRC/A6XR	Headquarters Air Force Reserve Command Director of Communications Planning and Budget Execution Branch
HQ AFRC/PKA	Headquarters Air Force Reserve Command Acquisition Management Branch
HQ AFRC/IP	Headquarters Air Force Reserve Command Director of Information Protection Office
HQ ARPC	Headquarters Air Reserve Personnel Center
HT	Hub Transport
HTML	Hypertext Markup Language
IA	Information Assurance
IAO	Information Assurance Officer
IAW	In accordance with
IaaS	Infrastructure as a Service
ICM	Internal Control Measures
I-COOP	Interim Continuity of Operations Capability
IE	Internet Explorer (Microsoft)
IEEE	Institute of Electrical and Electronics Engineers
IMM	International Mail Manual
IMS	Integrated Master Schedule
INOSC	Integrated Network Operations and Security Center
INOSC-E	Integrated Network Operations and Security Center - East
IOS	Internal Operating System
IPN	Installation Processing Node
IPO	Information Protection Office
IPR	Internal Program Review
IPTV	Internet Protocol Television
IRAPT	Invoice, Acceptance, Receipt, and Property Transfer
ISDN	Integrated Services Digital Network
ISO	International Standards Organization
IT	Information Technology
i-TRM	Info-structure Technology Reference Model
ITS	Information Transport System
ITU	International Telecommunications Union
IUID	Item Unique Identification
IVR	Interactive Voice Response
IWS	Installation Warning System
JCIAAM	Joint Common Information Assurance Assessment Methodology
JDAWS	Joint Data Access Web Server
JER	Joint Ethics Regulation

JIE	Joint Information Enterprise
JITC	Joint Interoperability Test Command
JP	Joint Publication
JPAS	Joint Personnel Adjudication System
JTR	Joint Travel Regulation
KEYMAT	Keying Material
KPIs	Key Performance Indicators
LAN	Local Area Network
LMR	Land Mobile Radio
LRA	Local Registration Authority
MAJCOM	Major Command
MCCC	MAJCOM Communications Coordination Center
MCEB	Military Communications Electronic Board
MCSE	Microsoft ® Certified Systems Engineer
MFM	MAJCOM Functional Managers
MFS	Monthly Financial Summary
MIB	Management Information Base
MICT	Management Internal Control Toolset
MIL-STD	Military Standards
MPF	Military Personnel Flight
MS	Microsoft
MS SCCM	Microsoft System Center Configuration Manager
MTS	Monthly Technical Summary
NACLC	National Agency Check with Local Agency Check and Credit Check
NAS	Network Attached Storage
NAS	Naval Air Station
NCDS	Net-Centric Data Strategy
NCSC	National Computer Security Center
NDAA	National Defense Authorization Act
NESI	Net-centric Enterprise Solutions for Interoperability
NETOPS	Network Operations
NFS	Network File System
NIPR	Non-Secure Internet Protocol Router Network
NISPOM	National Industrial Security Program Operating Manual
NIST	National Institute of Standards and Technology
NLT	No Later Than
NSS	National Security Systems
NTIA	National Telecommunications and Information Administration
NTIS	National Telecommunications and Information Systems

O&M	Operations & Maintenance
OCI	Organizational Conflict of Interest
ODL	Other Direct Costs
ODS	Operational Data Store
OMB	Office of Management and Budget
OPR	Office of Primary Responsibility
OPSEC	Operations Security
OSHA	Occupational Safety and Health Administration
OV	Operations View
OWA	Outlook Web Access
PAA	Privileged Access Agreement
PC	Personal Computer
PFE	Premier Field Engineer
PGI	Procedures, Guidance, and Information
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
PM	Program Manager
PMO	Program Management Office
POC	Point of Contact
POE	Power over Ethernet
POP	Period of Performance
POV	Privately Owned Vehicle
PPIRS	Past Performance Information Retrieval System
PRM	Performance Reference Model
PWS	Performance Work Statement
QAP	Quality Assurance Personnel
QCP	Quality Control Plan
QOS	Quality of Service
RF	Radio Frequency
RFID	Radio Frequency Identification
RFP	Request for Proposal
RMA	Return Merchandise Authorization
RMF	Risk Management Framework
ROS	Report of Survey
SaaS	Software as a Service
SANS	Storage Area Network
SCCM	System Center Configuration Manager (Microsoft)
SCIF	Sensitive Compartmented Information Systems
SOA	Service Oriented Architecture
SOCE	Service Oriented Cloud Environment
SCOM	System Center Operations Manager

SCS	Spectrum Certification Software
SDC	Standard Desktop Configuration
SDDP	Service Development and Delivery Process
SFAF	Standard Frequency Action Format
SIP	Session Initiated Protocol
SIPR	Secure Internet Protocol Router Network
SLA	Service Level Agreements
SMB	Server Message Block (protocol)
SME	Subject Matter Expert
SMO	Security Management Office
SOP	Standard Operating Procedures
SQL	Structured Query Language
SSL	Secure Socket Layer
SSRS	SQL Server Reporting Services
StdV	Standard View
STIG	Security Technical Implementation Guide
STP	Spanning Tree Protocol
SV	Systems View
TASKORD	Tasking Orders
TASS	Trusted Associate Sponsorship System
TBA	Training Business Area
TCO	Telephone Control Officer
TDY	Temporary Duty
TFTP	Trivial File Transfer Protocol
TMG	Threat Management Gateway
TMT	Telecommunications Management System
TMS	Telecommunications Management System
TPOC	Technical Point of Contact
UC	Unified Capability
UCCX	Cisco Unified Call Center Express
UCMJ	Uniformed Code of Military Justice
UMD	Unit Manning Document
UMPR	Unit Manpower Personnel Roster
US	United States
USAF	United States Air Force
UTA	Unit Training Assembly
UTAPS	Unit Training Assembly Participation System
VDI	Virtual Desktop Infrastructure
VGSA	Visitor Group Security Agreement
VLAN	Virtual Local Area Network
VOIP	Voice Over Internet Protocol
VoSIP	Voice Over Secure Internet Protocol

VPS	Voice Protection System
VTC	Video Teleconferencing
WAN	Wide Area Network
WARNORDS	Warning Orders
WAWF	Wide Area Work Flow
WWW	World Wide Web

TABLE 2
PUBLICATIONS USED IN DAILY OPERATIONS

Below is a list of publications and forms that are applicable to this PWS. NOTE: They are not all inclusive and are subject to change as they are revised and/or as guidance changes. The Contractor shall follow the applicable publications and forms to the extent and in the manner specified. All publications and forms are available on either the Air Force E-Publishing Website (www.e-publishing.af.mil) or the internet. However, in the event a publication and/or form is not available, the Government representative will work to provide a copy of the particular publication and/or form to the Contractor. (For more guidance, refer to para 5.18.)

- Privacy Act of 1974
- Joint Publication (JP) 1-02, *Department of Defense Dictionary of Military and Associated Terms*
- Joint Vision 2020 (current version)
- DODM 4525.6-M, *DoD Postal Manual*
- DOD 4525.8-M, *DoD Official Mail Management*
- DODD 4630.05, *Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)*
- DoDI 4630.8, *Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)*
- DoDI 5000.2, *Operation of the Defense Acquisition System*
- DoDI 5120.4, *Department of Defense Newspapers, Magazines and Civilian Enterprise Publications*
- DOD 5200.1-R, *DoD Information Security Program*
- DoDM 5200.01V1, *DoD Information Security Program: Overview, Classification, and Declassification*
- DoDM 5200.01V2, *DoD Information Security Program: Marking of Classified Information*
- DoDM 5200.01V3, *DoD Information Security Program: Protection of Classified Information*
- DoDM 5200.01V4, *DoD Information Security Program: Controlled Unclassified Information*
- DoD 5200.2-R, *Personnel Security Program*
- DoD 5200.08-R, *Physical Security Program*

- DODI 5205.8, *Access to Classified Cryptographic Information*
- DoD 5220.00-M, *Data Sanitization Method*
- DoD 5220.22-M, *National Industrial Security Program Operating Manual & Sup 1*
- DoD 5220.22-R, *Department of Defense Industrial Security Program*
- DoDD 5200.28, *Security Requirements for Automated Information Systems (AIS)*
- DoDD 5230.9, *Clearance of DoD Information for Public Release*
- DoDD 5240.1, *Activities of DoD Intelligence Components that Affect United States Persons*
- DoDI 5200.40, *DoD Information Assurance Certification and Accreditation Process (DIACAP)*
- DoDD 5400.7, *DoD Freedom of Information Act Program*
- DoD 5400.11-R, *Department of Defense Privacy Program*
- DoDD 5400.11, *Department of Defense Privacy Program*
- DoD 5500.7-R, *Joint Ethics Regulation (JER)*
- DoD 7000.14-R, Volume 2A and 2B, *Department of Defense Financial Management Regulation*
- DoDD 8000.1, *Management of the Department of Defense Information Enterprise*
- DODD 8100.1, *Global Information Grid (GIG) Overarching Policy*
- DODD 8100.2, *Use of Commercial Wireless Devices, Services, and Technologies in the DoD Global Information Grid (GIG)*
- DoDI 8100.3, *Department of Defense (DoD) Voice Networks*
- DoDD 8140, Cyberspace Workforce Management
- DODD 8320.02, *Data Sharing in a Net-Centric Department of Defense*
- DoDD 8320.2, *Information Sharing in a Net-Centric Department of Defense* (current version)
- DODI 8320.04, *Item Unique Identification (IUID) Standards for Tangible Personal Property*
- DoDD 8500.1, *Information Assurance*
- DoDD 8500.2, *Information Assurance Implementation*
- DoDI 8510.01, *DoD Information Assurance Certification and Accreditation Process (DIACAP)*
- DoDD 8570.01M, *Information Assurance Workforce Improvement Program (will be replaced by* DoDD 8140, Cyberspace Workforce Management)
- DoD 8910.1-M, *DoD Procedures for Management of Information Requirements*
- DoDD 8910.1-M, *DoD Procedures for Management of Information Requirements*
- DoD Radio Frequency Identification (RFID) Policy Memo, 30 Jul 2004
- Chairman of the Joint Chiefs of Staff Manual (CJCSM) 3170.01C, *Operation of the Joint Capabilities Integration and Development System*
- Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3170.01G, *Joint Capabilities Integration and Development System (JCIDS)*
- CJCSI 6211.02C – *Defense Information System Network (DISN): Policy and Responsibilities*

- CJCSI 6211.02D, *Defense Information Systems Network (DISN) Responsibilities*
- CJCSI 6215.01, *Policy for the Defense Switched Network*
- CJCSI 6212.01E, *Interoperability and Supportability of Information Technology and National Security Systems*
- CJCSI 6510.01, series, *Defense-in-Depth: Information Assurance (IA) and Computer Network Defense (CND)*
- AFPD 10-7, *Information Operations*
- AFI 10-701, *Operations Security (OPSEC)*
- AFI 10-712, *Telecommunications Monitoring and Assessment Program (TMAP)*
- AFMAN 14-304, *The Security, Use and Dissemination of Sensitive Compartmented Information (FOUO)*
- AFPD 16-2, *Disclosure of Military Information to Foreign Governments and International Organizations*
- AFI 14-1404, *Air Force Information Security Program*
- AFI 16-1406, *Air Force Industrial Security Program*
- AFMAN 23-110V2, *USAF Supply Manual*
- AFI 23-111, *Management of Government Property in Possession of the Air Force*
- AFMAN 23-220, *Reports of Survey for Air Force Property*
- AFI 24-301, *Vehicle Operations*
- AFPD 33-1, *Cyberspace Support*
- AFI 31-101, *Integrated Defense*
- AFI 31-113, *Installation Perimeter Control*
- AFI 31-401, *Air Force Information Security Program*
- AFI 31-501, *Personnel Security Program Management*
- AFI 31-601, *Industrial Security Program Management*
- AFI 33-106, *Managing High Frequency Radios, Personal Wireless Communication Systems, and the Military Affiliate Radio System*
- AFI 33-112, *Information Technology Hardware Asset Management*
- AFMAN 17-1203 Information Technology (IT) Asset Management (ITAM)
- AFI 33-115V1, *Network Operations (NETOPS)*
- AFI 33-115V2, *Licensing Network Users and Certifying Network Professionals*
- AFI 33-115V3, *Air Force Network Operating Instruction*
- AFI 33-116, *Long-Haul Telecommunications Management*
- AFI 33-119, *Air Force Messaging*
- AFI 33-127, *Electronic Messaging Registration and Authority*
- AFI 33-129, *Web Management and Internet Use*
- AFI 33-150, *Management of Cyberspace Support Activities*
- AFMAN 33-152, *User Responsibilities and Guidance for Information System*s
- AFPD 33-2, *Information Assurance (IA) Program*
- AFI 33-200, *Information Assurance Management*
- AFI 33-201V1, *Communications Security (COMSEC)(FOUO)*
- AFI 33-201V2, *Communications Security (COMSEC) User Requirements (FOUO)*

- AFI 33-201V4, *Cryptographic Access Program (FOUO)*
- AFI 33-201V5, *Controlled Cryptographic Items (CCI)(FOUO)*
- AFI 33-201V7, *Management of Manual Cryptosystems (FOUO)*
- AFI 33-201V9, *Operational Instructions for Secure Voice Devices (FOUO)*
- AFI 33-210, *AF Certification and Accreditation (C&A) Program (AFCAP)*
- AFI 33-230, *Information Assurance Assessment and Assistance Program*
- AFI 33-214V1, *(S) Emission Security Assessment*
- AFI 33-215, *Controlling Authorities for COMSEC Keying Material (KEYMAT)*
- AFI 33-217, *Voice Call Sign Program*
- AFMAN 33-282, *Computer Security (COMSEC)*
- AFMAN 33-285, *Information Assurance (IA) Workforce Improvement Management*
- AFMAN 33-402, Service Development and Delivery Process (SDDP)
- AFPD 33-3, *Information Management*
- AFI 33-322, *Records Management Program*
- AFI 33-324, *The Air Force Information Collections and Reports Management Program*
- AFMAN 33-326, *Preparing Official Communications*
- AFI 33-332, *Air Force Privacy Program*
- AFH 33-337, *The Tongue and Quill*
- AFMAN 33-363, *Management of Records*
- AFI 33-364, *Records Disposition-Procedures and Responsibilities*
- AFI 33-580, *Spectrum Management*
- AFI 35-109, *Visual Information*
- AFI 38-501, *Air Force Survey Program*
- AFI 40-102, *Tobacco Use in the Air Force*
- AFPD 61-2, *Management of Scientific and Technical Information*
- AFI 61-204, *Disseminating Scientific and Technical Information*
- AFI 63-1201, *Life Cycle Systems Engineering*
- AFI 65-503, *US Air Force Cost and Planning Factors*
- AFI 71-101V2, *Protective Service Matters*
- AFI 91-202, *The US Air Force Mishap Prevention Program*
- AFI 91-203, *Air Force Consolidated Safety Instruction (*paragraphs 6.2.1, 6.2.16 and 6.2.17)
- AFI 91-204, *Safety Investigation & Reports*
- AFRIMS (Air Force Records Information Management System), website located at Robins
- AFBI 32-2001, *Fire Protection Operations & Fire Prevention Program (applies for on-site performance at Robins AFB only)*
- Occupational Safety and Health Administration Standards (OSHA)
- TO 00-35D-54, *US Air Force Deficiency Reporting, Investigation, and Resolution (DRI&R) process*

- TO 00-33A-1001, *Technical Manual, Methods and Procedures: General Communications Activities Management Procedures and Practice Requirements*
- Allied Communications Publication (ACP) 123(A), *Common Messaging Strategy and Procedures*
- ACP 133, *Common Directory Services and Procedures*
- ACP 134, *Telephone Switchboard Operating Procedures*
- AFKAG-1, *Communications Security (COMSEC) Operations*
- AFKAG-2, *Air Force COMSEC Accounting Manual*
- AFSSI 5004V1, *The Certification and Accreditation (C&A) Process*
- AFSSI 5009, *Information Protection (IP) Interim Toolset*
- AFSSI 5020, *Remanence Security* ***(converts to AFMAN 33-224)***
- AFSSI 5021, *Vulnerability and Incident Reporting* ***(converts to AFMAN 33-225v2)***
- AFSSM 5022, *Network Risafssik Analysis Guide*
- AFSSI 5023, *Virus and Other Forms of Malicious Logic*
- AFSSI 5024V3, *The Designated Approving Authorities Handbook*
- AFSSI 7010, (S) Emission Security Assessment **(will convert to AFMAN 33-214V1)**
- AFSSI 7700, *Emission Security (EMSEC)*
- Air Force FAR Supplement (AFFARS)
- CIAC-2305 R.1, *UNIX Incident Guide: How to Detect an Intrusion*
- CSC-STD-002-85, *Department of Defense Password Management Guideline*
- Director of Central Intelligence Directive (DCID) 1/21, *Physical Security Standards for Sensitive Compartmented Information Facilities (SCIF)*
- Executive Order 12958, *Classified National Security Information*
- Federal Information Processing Standards (FIPS)
- FIPS) Publication 48, *Guidelines on Evaluation of Techniques for Automated Personal Identification*
- FIPS Publication 83, *Guideline on User Authentication Techniques for Computer Network Access Control*
- FIPS Pub 140-2, *Security Requirements for Cryptographic Modules*
- FIPS Pub 192, *Application Profile for the Government Information Locator Service (GILS)*
- Public Law 96-511, *The Paperwork Reduction Act of 1980, as amended 1986, Title 44, United States Code, Chap 35*
- Public Law 100-235, *Computer Security Act of 1987*
- National Telecommunications and Information Systems (NTIS) Security Directive No. 600, *Communications Security (COMSEC) Monitoring*
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-55, Guide to *Information Technology Security Services*
- NCSC-TG-017, *A Guide to Understanding Identification & Authentication in Trusted Systems*

- Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources*
- STIGS (DoD Security Technical Implementation Guides) and Checklists
- USCyber Orders
- Information Assurance Vulnerability Notices
- AF IT Lean Reengineering and SISSU Guidebook v5.0, (current version)
- American National Standards Institute (ANSI) Documents
- ANSI/TIA/EIA-568-A, Commercial Building Telecommunications Cabling Standard
- ANSI/TIA/EIA-568-A-1 Propagation Delay and Delay Skew Specifications for 100 4-pair Cable
- ANSI/TIA/EIA-569-1990, Commercial Building Standard for Telecommunications Pathways and Spaces
- TIA/EIA Standard-SP-3490 DRAFT 11, Residential Telecommunications Cabling Standard
- ANSI/TIA/EIA-606-1993, Administration Standard for the Telecommunications Infrastructure of Commercial Building
- ANSI/TIA/EIA-607-1994, Commercial Building Grounding and Bonding Requirements for Telecommunications
- CAM 09-39
- Combat Information Transport System (CITS) – Information Transport System (ITS) Architecture
- Computer Fraud and Abuse Act of 1986
- CND Directives as directed by USCYBERCOM
- Code of Federal Regulations (CFRs)
- Data Interchange Standards Community (E-Business)
- Defense Federal Acquisition Regulation Supplement (DFARS)
- Defense Information Systems Agency ATM and Voice Specification Standards
- DFARs and Procedures, Guidance, and Information (PGI)
- DISA Circular 310-M70-87, *Methods and Procedures Operational Policies and Procedures for the Defense Messaging System (DMS)*
- DISA Concept of Operations (CONOPS)
- DISA and CSIP (Cyber Security Inspection Program)
- DISA STIG, *Application Security and Development*
- DOD CIO Memorandum, *Department of Defense Information System Standard Consent Banner and User Agreement, 9 May 08*
- DoD CIO Department of Defense Net-Centric Data Strategy, 9 May 2003
- DoD Discovery Metadata Specification (DDMS Version; (current version)
- DoD Enterprise Architecture (EA) Data Reference Model (DRM) DoD Enterprise Architecture Technical Reference Model
- DoD IPv6 Memorandum, June 9, 2003, and DoD CIO IPv6 Memorandum, 29 September 2003
- DoD IPv6 Generic Test Plan, Version 3

- DoD IPv6 Standards Profiles for IPv6 Capable Products, Version 2 DoD IT Standards Registry (DISR)
- DoD Open Technology Development Guidebook
- Electronic Industries Association (EIA) Standards
- Electronic Industries Association (Alliance)
- Federal Acquisition Regulation (FAR)
- Federal Telecommunications Recommendation 1090-1997, Commercial Building Telecommunications Cabling
- Global Information Grid (GIG)
- Info-structure Technology Reference Model (i-TRM)
- Industry Best Practices in Achieving Service Oriented Architecture (SOA), 22 April 2005
- Institute of Electrical and Electronics Engineers (IEEE) Standards
- International Standards Organization (ISO) Documents
- International Committee for Information Technology Standards
- International Telecommunications Union ITU
- Joint Common Information Assurance Assessment Methodology (JCIAAM)
- Joint DoD/Department of National Intelligence (DNI) Federated Search Specification
- Joint Interoperability Test Command (JITC) Requirements
- JTF-GNOP WARNORD 07-37, Public Key Infrastructure Implementation Phase 2 (current version)
- Military Standards, Specifications, and Regulations (MIL-STDs, DoD-STDs)
- National Computer Security Center (NCSC) Documents
- National Institute for Standards and Technology (NIST) (formerly National Bureau of Standards, NBS) Documents
- National Security Agency Guidelines
- National Security Agency Rainbow Series
- Net-centric Enterprise Solutions for Interoperability (NESI)
- Net-Centric Operations & Warfare Reference Model
- Net-Centric Data Strategy (NCDS)
- NIST Special Publication 800-5, *Guide to the Selection of Anti-Virus Tools and Techniques*
- OASD Net-Centric Checklist, Ver. 2.1.3, 12 May 2004
- OMB 95-01, *Establishment of the Government Information Locator Service*
- Security Technical Implementation Guides (STIGS)
- SMI-ELS Strategic Concept V1, 1 September 2009
- Tasking Orders (TASKORDS)
- The Common Criteria Evaluation and Validation Scheme TIA/EIA-TSB-67, Transmission Performance Specifications for Field testing of Unshielded Twisted-Pair Cabling Systems
- TIA/EIA-TSB-72, Centralized Optical Fiber Cabling Guidelines
- TIA/EIA-TSB-75, Additional Horizontal Cabling Practices for Open Offices

- Title 5, Code of Federal Regulations, Part 1320, *Controlling Paperwork Burdens on the Public*
- TL9000 Quality Management System QuEST Forum
- Uniform Code of Military Justice (UCMJ), Article 92
- USAF Black Voice Switching Systems Strategy
- USAF Black Voice Switching System Profile
- Warning Orders (WARNORDS)

FORMS USED IN DAILY OPERATIONS

DEPARTMENT OF DEFENSE FORMS

DD 254	DoD Contract Security Classification Specifications
DD 1172-2	Application for Identification Card/DEERs Enrollment

AIR FORCE FORMS

AF 9	Request for Purchase
AF 649	Verification of Long Distance Telephone Calls
AF 833	Multimedia Work Order
AF 1297	Temporary Issue Receipt
AF 2005	Issue/Turn-In Request
AF 2583	Request for Personnel Security Action
AF 2586	Unescorted Entry Authorization Certificate
AF 2587	Security Termination Statement
AFCOMSEC 9	Cryptographic Access Certificate (PA) (FOUO)
AFCOMSEC 16	COMSEC Account Daily Shift Inventory
AFTO 95	Significant Historical Data

STANDARD FORMS

SF 85P	Questionnaire for Public Trust Positions
FD 258	Fingerprint Card
SF 312	Classified Information Nondisclosure Agreement
SF 701	Activity Security Checklists

TABLE 3
FIELD LOCATIONS AND TYPE OF IT SUPPORT

Location	AFRC Host Base Cyber Trans (3.4.6.)	AFRC Host Base PKI/LRA (3.4.15.)	AFRC Host Base CPF Comm (3.7.1.)	Base CSC (3.7.2.)	Server Support (3.7.3.)	HQ USAF/RE VTC Facilitator (3.8.3.4.)
ARPC – Buckley AFB, CO	X		X			
Pentagon – Washington D.C.						X
301 FW – NAS-JRB Ft Worth, TX	X	X	X	X	X	
304 RQS – Portland IAP, OR			X		X	
434 ARW – Grissom ARB, IN	X	X	X	X	X	
439 AW – Westover ARB, MA	X	X	X	X	X	
919 CS – Duke Field, FL	X				X	
452 AW – March ARB, CA	X	X	X	X	X	
482 FW – Homestead ARB, FL	X	X	X	X	X	
910 AW – Youngstown ARB, OH	X	X	X	X	X	
911 AW – Pittsburgh ARS, PA	X	X	X	X	X	

TABLE 4
HQ AFRC AND TYPE OF IT SUPPORT (Robins AFB, GA)

Location	Server Support (3.4.4.; 3.4.5.; 3.4.7.; 3.4.12., 3.4.13., 3.4.14., 3.4.16., 3.4.17., 3.7.3.)	Cyber Trans (3.4.8.)	Enterprise Network Infra (3.4.9., 3.4.10., 3.4.11., 2.7.)	CPF (3.7.1.)	Base CSC (3.7.2.)	PKI/LRA (3.4.15.)	VTC (3.8.)	Virtual (3.4.3.)	DBA Admin (3.4.4.)	Program Mgmt (2.1. thru 2.8.; 3.4.2.)	Support (2.10., 2.11., 2.12., 2.13., 3.6., 3.7.2., 3.9., 3.10.)
AFRC – Robins AFB, GA	X	X	X	X	X	X	X	X	X	X	X

TABLE 5
POPULATION AND WORKSTATIONS/SERVERS SUPPORTED
As of: 17 Jan 2017

LOCATION	POPU-LATION	# WORK-STATIONS (NIPR)	# SERVERS BY DISTINGUISHED NAME (NIPR)	# WORK-STATIONS (SIPR)	# VIRTUAL SERVERS (SIPR	# USERS (SIPR)
HQ AFRC – Robins AFB, GA	1,724	2,118	450	383	35	626
HQ ARPC – Buckley AFB, CO	423	601	36	0	0	0
94 AW – Dobbins ARB, GA (In-sourced, MSE and ASE support only; no on base support)	2,027	1,727	92	33	0	139
301 FW – NAS-JRB Ft Worth, TX	1,905	1,548	111	31	0	156
304 RQS – Portland IAP, OR	118	160	5	5	0	20
434 ARW – Grissom ARB, IN	1,769	1,599	44	31	0	112
439 AW – Westover ARB, MA	2,523	1,678	42	18	0	136
452 AW – March ARB, CA	3,730	2,711	133	50	0	212
482 FW – Homestead ARB, FL	1,981	1,536	49	71	0	120
910 AW – Youngstown ARB, OH	1,447	1,204	49	13	0	92
911 AW – Pittsburgh ARS, PA	1,194	1,019	75	13	0	147
914 AW – Niagara Falls AFS, NY (In-sourced, MSE and ASE support only; no on base support)	1,425	1,127	71	19	0	140
919 SOW – Duke Field, FL	869	1,059	8	0	0	0
934 AW – Minn-St Paul, MN (In-sourced, MSE and ASE support only; no on-base support)	1,453	1,133	50	26	0	164
Total Population Supported	**22,588**	**19,220**	**1,215**	**693**	**35**	**2,064**