Logo

Description automatically generated

U.S. Department of State

Evolve

Attachment J-32

Sample Task Order

for

Network Services

SOLICITATION  
19AQMM22R0029

**OCTOBER 2022**

**Table of Contents**

[1.0 General 9](#_Toc116298677)

[1.1 Network Services Overview 9](#_Toc116298678)

[1.2 DOS Strategic Goals 11](#_Toc116298679)

[1.3 Networking Services Strategic Goals 12](#_Toc116298680)

[1.4 Scope 13](#_Toc116298681)

[1.4.1 Scope of the Service Environment to Be Supported 13](#_Toc116298682)

[1.4.2 Current Networking Environments 13](#_Toc116298683)

[1.5 Technical Direction 14](#_Toc116298684)

[1.6 Policies and Procedures 14](#_Toc116298685)

[1.7 Personnel 14](#_Toc116298686)

[1.8 Government-Furnished Equipment / Information 15](#_Toc116298687)

[1.9 Travel 15](#_Toc116298688)

[1.10 Standard Work Hours 15](#_Toc116298689)

[1.11 Telework 16](#_Toc116298690)

[1.12 Performance Requirements 16](#_Toc116298691)

[1.13 Required Languages 17](#_Toc116298692)

[1.14 Government-Data 17](#_Toc116298693)

[1.15 Tools 17](#_Toc116298694)

[1.16 Network Hardware 18](#_Toc116298695)

[1.17 Transition Projects 18](#_Toc116298696)

[1.18 Constraints 19](#_Toc116298697)

[1.19 IT Compliance 19](#_Toc116298698)

[2.0 Network Services Requirements 20](#_Toc116298699)

[2.1 Common Network Service Requirements 20](#_Toc116298700)

[2.2 Network Engineering and Operations 20](#_Toc116298701)

[2.2.1 Engineering Design Support 20](#_Toc116298702)

[2.2.2 Worldwide VPN/Non-VPN Secure Connectivity Solutions Development 21](#_Toc116298703)

[2.2.3 Voice Over IP (VoIP) and Video Conferencing Support 21](#_Toc116298704)

[2.2.4 Deployment Support 21](#_Toc116298705)

[2.2.5 Core Infrastructure Toolset Management 22](#_Toc116298706)

[2.2.6 Wi-Fi Design and Engineering Services 22](#_Toc116298707)

[2.2.7 Regional Relay Facility - Network Engineering 24](#_Toc116298708)

[2.2.8 Operations Center Support 25](#_Toc116298709)

[2.2.9 IT Service Management (ITSM): Tier III Network Support 25](#_Toc116298710)

[2.2.10 IT Service Management (ITSM): Tier II Network Support 26](#_Toc116298711)

[2.2.11 Centrally Monitored and Engineered Security Controls Support 27](#_Toc116298712)

[2.2.12 Regional Relay Facility Network Service Center - Network Monitoring 27](#_Toc116298713)

[2.2.13 Capacity Planning for Department Bandwidth Requirements 29](#_Toc116298714)

[2.2.14 Quality of Service (QoS) Support 29](#_Toc116298715)

[2.2.15 Wi-Fi Operations Services 30](#_Toc116298716)

[2.2.16 Contingency Planning Support 32](#_Toc116298717)

[2.3 Endpoint Engineering and Support 33](#_Toc116298718)

[2.3.1 Endpoint Engineering and Design 33](#_Toc116298719)

[2.3.2 Enterprise Software Packaging and Distribution (ESPD) 33](#_Toc116298720)

[2.3.3 Patch Management Support 34](#_Toc116298721)

[2.3.4 Systems Management Support (Microsoft’s Endpoint Configuration Manager (MECM)) 34](#_Toc116298722)

[2.3.5 Compliance 36](#_Toc116298723)

[2.3.6 Lifecycle Support 36](#_Toc116298724)

[2.4 Customer Facing Services 36](#_Toc116298725)

[2.4.1 24/7 x 365 IT Operations Center Support (ITOC) 36](#_Toc116298726)

[2.4.2 Regional Relay Facility Network Service Center (NSC) 38](#_Toc116298727)

[2.4.3 IT Change Control Board (ITCCB) Support 38](#_Toc116298728)

[2.5 Radio Communications 39](#_Toc116298729)

[2.5.1 Distributed Antenna System (DAS) 39](#_Toc116298730)

[2.6 Network & System Tools 40](#_Toc116298731)

[2.6.1 Security and Access Management Engineering 40](#_Toc116298732)

[2.6.2 Common Network & System Tools Requirements 41](#_Toc116298733)

[2.6.3 iPost Support 42](#_Toc116298734)

[2.7 Directory Services 42](#_Toc116298735)

[2.7.1 Directory Engineering Support 42](#_Toc116298736)

[2.8 Telecommunications Services 44](#_Toc116298737)

[2.8.1 Common Requirements 44](#_Toc116298738)

[2.8.2 Telephone / Telecommunications Engineering, Solutions, Systems, and Services 48](#_Toc116298739)

[2.9 Regional Relay Facility (RRF) Support 59](#_Toc116298740)

[2.9.1 General RRF Support Requirements 59](#_Toc116298741)

[2.9.2 Relay Infrastructure Management Support 60](#_Toc116298742)

[2.9.3 Regional Relay Facility Change Management and Data Center Management 60](#_Toc116298743)

[2.9.4 Network Services Center - Network Encryption Services 61](#_Toc116298744)

[2.9.5 COMSEC Office of Record services/COMSEC child account manager services 61](#_Toc116298745)

[2.9.6 COMSEC Inline Network Encryption (INE) Support 62](#_Toc116298746)

[2.9.7 COMSEC Secure Voice Terminal equipment Support 62](#_Toc116298747)

[2.10 Cybersecurity Management 62](#_Toc116298748)

[2.10.1 Cybersecurity Management Support 62](#_Toc116298749)

[2.10.2 Compliance and Reporting 63](#_Toc116298750)

[2.10.3 Cybersecurity Risk Management 64](#_Toc116298751)

[2.10.4 Access Management 65](#_Toc116298752)

[2.11 Data Warehouse, Business Intelligence and Asset Discovery 66](#_Toc116298753)

[2.11.1 Data Warehouse 66](#_Toc116298754)

[2.11.2 Business Intelligence 67](#_Toc116298755)

[2.11.3 Asset Discovery 67](#_Toc116298756)

[3.0 Acceptance Criteria and Inspection 67](#_Toc116298757)

[4.0 Transition Services 68](#_Toc116298758)

[4.1 Transition in Services 68](#_Toc116298759)

[4.2 Transition Out Services 68](#_Toc116298760)

[5.0 Key Personnel Requirements 68](#_Toc116298761)

[5.1 Program Manager 69](#_Toc116298762)

[5.2 Service Line Leads 70](#_Toc116298763)

[5.3 Network Manager 70](#_Toc116298764)

[5.4 Configuration Management Lead 71](#_Toc116298765)

[5.5 Directory Services Engineer 71](#_Toc116298766)

[5.6 Network Administrator 71](#_Toc116298767)

[5.7 Network Draftsman 72](#_Toc116298768)

[5.8 Network Installation Lead 72](#_Toc116298769)

[5.9 Endpoint Support Expert 73](#_Toc116298770)

[5.10 Wide Area Network Administrator 73](#_Toc116298771)

[5.11 Network Cybersecurity Lead 74](#_Toc116298772)

[5.12 Network Architect 74](#_Toc116298773)

[5.13 Unified Communications Network Architect 75](#_Toc116298774)

[5.14 WiFi Architect 75](#_Toc116298775)

[5.15 Change Management Lead/IT Requirements Lead 76](#_Toc116298776)

[5.16 Datacenter Infrastructure Management (DCIM) System Expert 76](#_Toc116298777)

[5.17 Communications Security (COMSEC) Expert 77](#_Toc116298778)

[5.18 Operations Manager 78](#_Toc116298779)

[5.19 Incident Manager 79](#_Toc116298780)

[5.20 Problem Manager 79](#_Toc116298781)

[5.21 System Administrator (REACH) 80](#_Toc116298782)

[6.0 Labor Categories 80](#_Toc116298783)

[6.1 Pricing Table 81](#_Toc116298784)

[7.0 Task Order Deliverables 132](#_Toc116298882)

[7.1 Task Order Monthly Status Reports (MSR) 132](#_Toc116298883)

[7.2 Labor allocation report (Timesheets) 132](#_Toc116298884)

[7.3 Service and Incident Reports 133](#_Toc116298885)

[7.4 Meeting minutes 133](#_Toc116298886)

[8.0 Evaluation Criteria 134](#_Toc116298887)

[8.1 Employee Technical Performance 134](#_Toc116298888)

[8.2 Employee Customer Service 134](#_Toc116298889)

[8.3 Project Management 134](#_Toc116298890)

[8.4 Staffing Management 134](#_Toc116298891)

[Section 11: Performance Measurement 135](#_Toc116298892)

[11.1 Operational Metrics 135](#_Toc116298893)

# General

## Introduction

This Performance Work Statement (or “PWS”) sets forth the roles and responsibilities of the Parties for the Network Services provided under the Evolve IDIQ as part of the Network and Telecom Services functional category.

## DOS Strategic Goals

We are committed to providing the enterprise with high availability for its mission-critical applications through joint engineering of the next generation of digital communications infrastructure for 280 posts and offices worldwide. The objective of this PWS is for DOS to obtain technical expertise and scalable support to:

* Provide the Department with a secure global network and infrastructure safe from intentional attack, engineered and designed to never trust and always verify
* Improve network availability and reliability
* Enhance customer response times through a comprehensive and efficient approach to providing network services

This directly supports the goals defined within our DOS Information Technology Strategic Plan FY 2019 – 2022 Excerpt from DOS Information Technology Strategic Plan FY 2019 – 2022.

As the global technology landscape evolves, our diplomats expect integration of the latest IT tools into their working lives. The influx of new technology must enable the conduct of diplomacy and must connect people to the information they need when they need it. DOS strategic goals and guiding principles are highlighted below.

*Goal 1: Data as a Strategic Asset*

Managing and leveraging data is integral to DOS’s mission and operation. We will invest in data over the coming years as a strategic asset. Our data represents a true, long-term asset of value, and in most cases, our data will outlive the useful life of our technologies.

*Goal 2: Enhanced User and Mission Effectiveness*

The influx of new technology makes it possible for employees to communicate, collaborate, and work more efficiently. DOS will aggressively move to leverage innovative and emerging services to provide our employees ready access to the tools and information resources that are crucial to their work. Our workforce will be empowered through rapid deployment of innovative technologies and remote capabilities.

*Goal 3: IT Modernization*

The IT Modernization goal outlines the Department’s migration to the cloud, cybersecurity efforts, and legacy IT systems modernization that will transform IT. DOS will work rapidly to achieve the President’s IT modernization vision and to comply with new and existing federal mandates.

*Goal 4: Strengthened IT Management*

This goal focuses on the best practices needed to transform the way IT is managed and delivered at DOS in support of our diplomatic and development mission.

## Networking Services Strategic Goals

Following the DoS Strategic Guiding Principles, the DOS network services organization has developed the 2020-2025 Networking Strategic Plan using the DoS Strategic Plan, the IRM Strategic Plan, previous Networking Strategic Plans, and common business drivers as inputs.

DOS network services leadership worked to develop a tailored and relevant mission statement that would summarize the aims and values of the organization. It likewise developed a vision statement to describe DOS desired future state for networking. DOS network services leadership and staff then worked together to develop goals and objectives that would help it carry out its mission and work towards its vision. The result of these efforts is the Networking Strategic Plan, which provides a five-year roadmap. Annual tactical planning efforts identify the work that will be done over the next three years to implement the strategy

| **DOS Networking Strategic Goals** | **Strategic Objectives** |
| --- | --- |
| I. State of the art reliable, and secure IT solutions and infrastructure to the Department of State and its partnering agencies | 1.1: Provide network infrastructure and service that is consistent, resilient, reliable, and modern. |
| 1.2: Provide and support interoperable multi-platform cloud ecosystem. |
| 1.3: Collect information about our customers’ mobility needs and provide on-demand access to meet these needs. |
| II: Operate as a service-oriented organization | 2.1: Frequently gather data to measure our performance against customers' needs and satisfaction. |
| 2.2: Understand the long-term changes in customers’ requirements and what’s required to meet them. |
| 2.3: Provide consistent, coordinated, and predictable customer service. |
| 2.4: Communicate DOS Network Services’ performance standards and procedures internally within the organization and measure performance against the established baseline |
| 2.5: Realize the full capabilities of assets, tools, and people and continuously evaluate performance. |
| III: Uphold security as the foundation to all IT solutions | 3.1: Implement a Zero Trust architecture to transform the network in the next five years. |
| 3.2: Design, build, and implement an Enterprise Identity Management System and access management architecture. |
| 3.3: Establish an Enterprise Risk Management function that consolidates and standardizes DOS Network Services’ Risk Management Functions and responsibilities. |
| 3.4: Increase Communications with DOS Network Services Partner Offices and customers to ensure that service upgrades (i.e., IT Security) is not impacting operational performance. |
| IV: Modernize infrastructure and security solutions that enable and enhance mission readiness | 4.1: Modernize legacy systems and supporting infrastructure and modernize the voice/data infrastructure in the next five years. |
| 4.2: Develop and provide the tailored tools, devices, and standards needed by the Enterprise for its mission. |
| V: Invest in our Network Services Resources | 5.1: Establish DOS Network Services’ core values. |
| 5.2: Develop and establish DOS Network Services’ human capital strategy. |
| VI: Manage and mitigate existential and institutional risks, inefficiency, and distraction (bureaucracy) | 6.1: Develop strategy, methodologies, and processes to identify, address, and mitigate existential and institutional risks, inefficiencies, and distractions. |

## Scope

Network Services are the services and activities as described in this Performance Work Statement. Vendor responsibilities include, but are not limited to, providing operational, administrative, management, and engineering support for the following DOS networks:

* OpenNet, the DOS sensitive but unclassified (SBU) network
* ClassNet, the DOS classified network
* Transport Only Network (TrON)
* State Optical Core (SOC),
* ONYX, the Diplomatic Telecommunications Service Program Office (DTS-PO) provisioned network supporting DOS and Other Government Agencies (OGA) as well as the successor to ONYX, Black Mountain
* DEVNet, the DOS development network
* Other unclassified wired and wireless networks including Dedicated Internet Networks (DINs)
* Interface to the Red Switch network
* Interconnections to the DOS multi-cloud environment

The scope of network operations includes:

* **Common Network Service Requirements**: Describes shared expectations across all services provided within this Performance Work Statement from strategic support to day-to-day activities.
* **Network Engineering and Design**: Architects, designs, deploys, and supports network solutions that are secure and maximize performance for classified and unclassified, wired, and wireless, communications and computing network users. Responsibilities include monitoring, supporting, and maximizing network and application performance, engineering major system enhancements for the Enterprise network infrastructures, and providing a security architecture that supports multi-level security across the Enterprise.
* **Network Operations**: Ensures the reliable operations and performance of DOS systems and network services by providing operational, administrative, and management support through the Department’s Enterprise Network Management Operations Center (ENMOC). Provides operational support for the Department’s server and client operating systems and technical support and coordination for detecting and correcting IT security vulnerabilities.
* **Standard Operating Environment**: Manages changes to the environment (e.g., operating systems, applications), provides lifecycle support for the network as well as security and access management tools, supports the IT Change Control Board (ITCCB) process, and defines/refines processes as needed.
* **Network and System Tools**: Provides oversight, lifecycle support and operations and maintenance for tools (e.g., monitoring, configuration, administration, security, access management) used to ensure network availability and security.
* **Regional Relay Facility (RRF) Support**: Regional Relay Facility (RRF) Support responsibilities ensure that the IT systems and substructure within the Region Relay Facility (RRF) Telecommunications Center Facility (TCF) hosting vital networking and Telecommunications assets for Department of State (DOS) and its OGA partners [ex. DTS-PO, Department of Defense (DoD), Department of Homeland Security (DHS), etc.] remain sufficiently secure, robust, scalable, and efficient to deliver integrated services throughout the underlying physical environment. This contributes to the readiness of systems and availability of physical resources that maintain the continuity of operations for DOS and OGA Relay systems and networks supporting vital missions around the globe.
* **Cyber Security Management**: Provides compliance and reporting, risk management, and access management centrally. Compliance and reporting encompass the guidance and standards developed by the National Institute of Standards and Technology (NIST) in compliance with the Federal Information Security Modernization Act (FISMA). Risk management deals with identifying and prioritizing risks to minimize the impact of vulnerabilities and to ensure the proper configuration of information systems. Finally, access management is the selective restriction of permissions to a network or local resource via policies and controls.
* **Data Warehouse, Business Intelligence and Asset Discovery**: Facilitates the storage and processing of structured and unstructured data for query, analysis, inventory, and reporting purposes. Data warehouses and the data they contain are carefully planned and assembled to deliver specific business analysis and decision-making results. Data warehousing and Asset Discovery will focus on centralized data storage of while business intelligence is concerned with data analysis and presentation. Accommodations must be made for the various types of structured and unstructured data, the technologies supporting the data and where the data is stored, whether state-hosted (on-premises, device, and applications), mobile, endpoints or outsourced (cloud containers).
* **Transition Services**: Describes activities such as transition planning, knowledge transfer, etc. required to successfully handoff ownership from the outgoing vendor to the incoming vendor and/or to DOS.
* **Telecommunications**: Provides, modernizes, and coordinates best in class telecommunication infrastructure engineering, solutions, services, and Government-wide Acquisitions Contract (GWAC) services to U.S. DOS bureaus, offices, posts, and inter-agency partners engaged with installation, operations, maintenance, and modernization for domestic and overseas telephonic, and telecommunications infrastructure, as well as the Distributed Antenna System engineering, solutions, and services.
* **Infrastructure Installation and Management**: Performs a variety of equipment and infrastructure maintenance tasks as part of operations support. These include installation/de-installation of networking/security devices, distribution-cabling systems (e.g., backbone fiber/copper cabling and connectors, distribution patch panels, network connection boxes, associated conduit systems), communication cabinets/racks, and other related mounting hardware. Other essential related tasks include completing and documenting preventive maintenance and/or infrastructure remediation activities (ex. infrastructure & cabling termination/repair/correction; periodic testing, equipment cabinet clean up, etc.) necessary for maintaining network performance, preserving capacity, ensuring the reliability of infrastructure, and resolving issues/failures.

## Current Service Environment

This section describes and scopes the network environment to be supported and complied with. These Service Environment Appendices are maintained by Vendor, reviewed with DOS, updated by Vendor, and made available to DOS on a quarterly basis.

### Current Networking Environments

The scope and scale of Networking Services to be provided under this PWS are addressed in the list below detailing service types and estimated service units provided across DOS networking environments:

Support includes, but are not limited to, the following locations:

* Washington Metro Area DOS facilities
* USUN Mission, New York, NY
* Charleston Financial Service Center, Charleston, SC
* Florida Regional Center, Fort Lauderdale, FL
* Passport Agencies throughout US states and territories
* National Processing Information Center II, Lansing, MI
* National VISA Center, Portsmouth, NH
* Kentucky Consular Center (KCC), Williamsburg, KY
* Office of Foreign Missions
* DS Field and Resident Offices
* United States Trade and Development Agency (USTDA) (including WiFi support)
* Blair House (including WiFi support)
* USAID
* Peace Corp
* Other government agencies

Overseas support includes, but are not limited to, the following locations. Note that overseas work will generally be only limited or short-term travel to support specific requirements.

* All US Embassies, Consulates, and Missions
* American Presence Posts
* Other locations with USG presence

### Tools

DOS currently uses the following tools to support delivery of network services and integrate with DOS IT Service Management processes:

* 1E Nomad
* Apptio
* Cacti
* Change Auditor
* Cisco Secure ACS
* Cisco Identity Service Engine (ISE)
* Cisco Smart Software Manager (CSSM)
* CiscoWorks (Campus Manager)
* Computer-aided design (CAD)
* CyberArk
* DS-RADAR
* Ekahau
* Entrust Security Manager
* HP OpenView
* HPNA
* InfoBlox Grid Manager iPost
* LiveAction (Netflow)
* Marconi’s Service on Data
* Microfocus Network Automation (MFNA)
* Microsoft EndPoint Configuration Manager
* Microsoft Project
* NetIQ Security Manager
* Netplus
* NeuralStar
* NightWatchman
* NIKSUN (NetVCR)
* NIKSUN NetX
* Okta
* Post Admin Tool (PAT),
* Radiant Logic
* RSA SecurID
* SailPoint
* ServiceNow Change Management ServiceNow Configuration Management Database (CMDB)
* ServiceNow Discovery
* ServiceNow Incident Management
* SmokePing
* Splunk
* Sunbird Data Center Infrastructure Management [DCIM] Software (dcTrack and PowerIQ)
* Systems Center Operations Manager (SCOM)
* RedSeal
* Tavve
* Visio
* VMware

### Network Hardware

DOS currently uses the following hardware as the primary means to provide network services:

* Hardware for Network Services
* Forcepoint
* Palo Alto
* Cisco ESA
* A10
* F5
* CISCO routers and switches (multiple models)
* ACCEDIAN test platform
* INFOBLOX

In addition, the DOS currently includes the following hardware that is being retired as part of the lifecycle replacement program:

****

### Transition Projects

The Vendor shall execute and complete specified projects that are either in flight or are planned. Such projects are the responsibility of the Vendor to complete as part of the Transition activities, in accordance with time frames specified by DOS. All projects use Agile methodology.

* Federal Zero Trust Architecture (ZTA) design and implementation
* Network Modernization- leveraging zero trust principles to modernize the Department’s primary method of connecting to the internet from the workplace, leveraging the Transport Only Network. Includes modernizing core infrastructure. Includes worldwide deployment of wireless access solutions.
* Network Mapping- deploying Red Seal to provide enterprise OpenNet maps, ingesting all domestic and overseas offices and posts.
* Cloud Access Security Broker- deploying a CASB to enhance security around cloud apps.
* Active Directory Redesign - modernizing the Department’s deployment of Microsoft’s Active Directory.

### Constraints

The following constraints apply to this task order.

The contractor shall:

* Comply with Government technical direction.
* Ensure all procurement documents and advisory assistance is in compliance with the Federal Acquisition Regulation (FAR), Department of State Acquisition Regulation (DOSAR), as well as other DOS standards, policies, procedures and guidelines and will comply with applicable international and country-specific laws, regulations and guidelines.
* Use the DOS Managing State Projects for Information Technology (MSP-IT) project management framework
* Demonstrate a high degree of experience at collaboration and coordination with Federal stakeholders and other Contractors.
* Not conduct themselves or convey information in a manner that will give the appearance the Contractor is a Government representative and/or is authorized to make decisions on behalf of the Government.
* Comply with all DOS guidelines, protect classified and sensitive information, and maintain accountability of government furnished equipment.
* Comply with any policies, processes, reporting requirements, etc..
* Be willing to perform in a fiscally constrained environment, characterized by uncertainty, which may result in the Government incrementally funding the contract.
* Work collaboratively with other Evolve vendors.

## IT Compliance

IT Compliance resources include setting policy, establishing controls, and measuring compliance to relevant legal and compliance requirements.

The Contractor shall:

* Comply with all relevant certification and accreditation requirements and documentation specified by DOS and the U.S. Government.
* Adhere to policies and procedures defined in the Foreign Affairs Manual (FAM) and associated Foreign Affairs Handbooks (FAHs) to include, but not limited to proactively reporting non-compliance issues and risks.
* Participate in compliance, risk and regulatory governing bodies, processes and activities as required.
* Measure (or provide inputs needed to support measurement of) compliance to relevant legal and compliance requirements.
* Monitor all work performed by assigned Contractor personnel to ensure the ongoing and continuous incorporation of and adherence to all appropriate Compliance requirements.
* Report on compliance in coordination with other DOS stakeholders and/or Contractors.
* Support remediation of compliance discrepancies as directed.
* Support the definition and establishment of controls to monitor compliance.

## Contract Type

This is a performance-based task order that utilizes Labor Hour Contract Line Items (CLINs).

# Network Services Requirements

Vendor shall be responsible for Network Services across DOS as described within this PWS. The following list identifies responsibilities.

## Performance Requirements

For all roles and responsibilities described herein, the contractor shall:

* Ensure all work activities are performed in a timely and cost-effective manner while maintaining the highest quality of performance to achieve expected outcomes.
* Ensure all work and tickets are recorded in the IT Service Management system unless specifically excluded at the direction of the Government lead.
* Use Agile project methodology for all projects unless specifically authorized otherwise.
* Document all processes utilized in the successful execution of operational, engineering, portfolio, program, or project activities.
* Ensure communications are thorough, accurate, timely, and tailored to the audience for both IRM stakeholders and the customer.
* When required, translate technical information into clear, readable content for use by business level and non-technical personnel.
* Organize, conduct, and attend meetings as required.
* Develop and deliver timely, complete, and accurate meeting artifacts as required.
* Use DOS designated repositories for all deliverables as required.
* Use international standards for IT management (such as ISO/IEC 20000) and document processes in a manner that can obtain and sustain certification, as required by DOS leadership
* Provide accurate timecards aligned to Government projects and codes

## Common Network Service Requirements

Common network service requirements describe expectations shared across all services provided. These include, but are not limited to:

* Providing strategy, planning, and support for network services day-to-day activities as well as projects
* Providing DOS-specific design guidance based on research and analysis, Industry best practices, inputs from DOS stakeholders, etc.
* Providing enterprise architecture services
* Using DOS-approved IT Service Management tools and processes to manage the end-to-end delivery of network services e.g., Incident Management, Problem Management, Inventory Management, Tier II & III support, using the ITSM system (i.e., ServiceNow) to manage incidents and service requests
* Managing DOS intranet sites
* Delivering reports and dashboards for agreed upon areas
* Maintain documentation in support of ISO20k certifications

## Network Engineering and Operations

Network engineering and operations are concerned with the development, deployment, sustainment, and retirement of network services for the entire Department.

### Engineering Design Support

* Define high level network strategies, service requirements, and policies.
* Provide internal and external network design and engineering to increase network speed, reliability, security, and availability.
* Investigate and implement network management tools to monitor the health of the network perimeters, incorporating redundant network design features to minimize outage and meet the State Department network objectives.
* Proactively identify network performance trouble spots and taking steps to fix before network outages, security incidents, or other performance issues occur.
* Implement a methodology for ensuring the availability and security of the Department’s networks by monitoring the global network perimeter infrastructures, identifying potential sources of congestion or conflict, and proactively eliminating potential network performance trouble spots.
* Support DOS efforts to design and implement the Federal Zero Trust Architecture (ZTA) strategy, potentially to include micro-segmentation and software defined networking (SDN), in coordination with the DOS cybersecurity organizations within IRM and DS and potentially with a Zero Trust program office.

### Worldwide VPN/Non-VPN Secure Connectivity Solutions Development

* Engineer and deploy VPN’s. The VPN can be used as Washington DC remote connections, or as local foreign post-to-post tail circuit connections or by other means as required.
* Engineer and deploy tail circuit encryption solutions for the VPN tail circuits.
* Provide design solutions that include non-VPN circuits and post-to-post serial links and deploy encryption solutions for all circuits.
* Connect a National Institute of Standards and Technology (NIST), Federal Information Processing Standards Publication (FIPS 140-2) approved level-two encryption device (currently using the CISCO product line) between the SBU network and the Internet Global Deployment.
* Ensure that the infrastructure will provide the added advantage of an alternative to the DTS-PO-provided circuit at each post and the ability to do future load balancing that will improve network efficiency and availability.
* Incorporate a backup infrastructure using the Internet, public telecommunication service, commercially available Very Small Aperture Terminal (VSAT) or other satellite services.
* Ensure network upgrades will provide DOS higher availability to their applications and more reliable network communications paths.

### Voice Over IP (VoIP) and Video Conferencing Support

* Evaluate, design, and implement new technologies for DOS networks, potentially to include IPv6, Voice Over IP telephony, video conferencing, Session Initiation Protocol (SIP), Session Boarder Controller (SBC), and Teams integration.

### Deployment Support

* Support the deployment efforts of designated DOS teams as coordinated by or with DOS, including, but not limited to scheduling resources, planning activities, implementation, installation, remote maintenance, security configuration, Tier II technical support, and other tasks in support of the deployment teams’ missions.
* Make contractor staff available for short-notice critical tasks, emergencies, and contingency operations.
* Develop transition and “Operations & Maintenance” documentation as part of planning activities.
* Perform local installation of core network and systems components and remote installation by telephonic assistance to diplomatic missions abroad, and subsequent completion by remote management.
* Apply security templates and configurations once components are installed.
* Provide Tier II support for core enterprise components once installed.

### Core Infrastructure Toolset Management

* Install all DOS provided hardware, operating systems, software, and patches in support of network and systems toolsets in accordance with DOS standards and configuration guidelines.
* Provide day-to-day operations of the core components of the network and systems toolsets through the use of approved management tools and established SOPs in order to ensure they are operational 24/7 x 365.
* Recommend upgrades or expansions of the core system servers as needed based on performance or other factors.
* Operate and maintain a tested backup system, network, and systems toolsets, including backing up the systems on a regularly scheduled basis to ensure no loss of data for more than twenty-four (24) hours.
* Develop and maintain custom knowledge scripts by which network and systems toolsets can report on applicable events relating to DOS’s enterprise network and systems devices worldwide.

### Wi-Fi Design and Engineering Services

* Design the Wi-Fi solution so that it shall support but not limited to: Internet of Things (IoT) and real time applications such as VOIP and video. Services include but are not limited to:
  + Wireless LAN Controllers (WLC): FIPS 140-2 (hardware and software) approved and Wi-Fi Alliance Certified; WLCs shall support the Institute of Electrical and Electronics Engineers (IEEE) 802.1, 802.3 and 802.11 standards; shall be capable of managing more than 10 WAPs simultaneously; shall be capable of being managed by Cisco Prime Infrastructure
  + Wireless Access Points (WAP): shall be FIPS 140-2 (hardware and software) approved and Wi-Fi Alliance Certified; support the IEEE 802.1 and 802.11 standards; shall be multi-radio capable for integrated Wireless Intrusion Detection System (WIDS) / Wireless Intrusion Prevention System (WIPS) capabilities; shall be able to operate in the 5GHz frequency band; shall be capable of being managed by Cisco Prime Infrastructure
  + Firewalls (FW): FIPS 140-2 (hardware and software) approved and meet Next Generation Firewall (NGFW) features such as but not limited to; stateful firewall, application visibility and control, intrusion prevention, advanced malware protection, and URL filtering; shall support automated policy application and enforcement; shall support a minimum throughput from 256 to 1750 Megabits per second (Mbps); shall support a minimum threat inspection from 125 to 1250 Mbps; shall be capable of being managed by Cisco FirePower Management Center or the next generation of management applications
  + Switches: 802.3af PoE+ standard at a minimum and be able to support at a minimum both a 10G copper and fiber backbone; shall be capable of being managed by Cisco Prime Infrastructure
* Provide telecommunication infrastructure to meet the customer’s Wi-Fi requirements and at minimum DOS and Industry standards. Telecommunications copper cabling for WAPs shall be CAT-6A or better. The telecommunications fiber cabling for backbone runs shall be OM3 or better.
* Provide FIPS 140-2 (hardware and software) approved encryption devices that meet DOS security and operational requirements.
* Site Surveys: Site activities include but are not limited to:
  + In Brief
  + Out Brief
  + Development of PRS
  + Site Preparation (e.g., Heating, Ventilation, and Air Conditioning (HVAC) enhancements, Electrical enhancements, Lightning Protection, Minor facility construction, Security enhancements, Penetrations, Telecommunication Infrastructure)
  + Planning and Engineering
  + Engineering Study (Use of only 5 GHz frequency, avoidance of installation in plenum-rated spaces (raised floor or above drop ceilings) and ceilings over 9 feet (10 feet max), WAPs for Conference rooms and CACs but should not be considered for design coverage for areas outside of the conference room, equipment installation and mounting so it is aesthetically pleasing and meets all DOS and Overseas Office Building (OBO) requirements, design so that Wi-Fi signals do not exceed the CAA signal strength limitation as specified in the current DS WLAN Security Standard for DIN and /or appropriate policies)
  + Cable Routing (e.g., cables that depart a CAA going out into a Non-CAA, as well as Cables that depart a CAA transit a Non-CAA and then re-enter a CAA shall meet all DOS security, safety, and operational requirements)
  + Scalability & Growth Analysis (Design the equipment and system for growth without the installation of additional equipment, shelves, or cabinets as determined by the site requirement. The installed hardware shall include a vacant slot capacity of minimum 10% for future use and minimum 10% on-site assignable growth spares)
* Design and implement systems that are interoperable with existing DOS, local, and commercial ISP infrastructure and equipment.
* Comply with the WLAN Standards for DIN, FAM, FAH, and the applicable sections of the DS Security Standards Handbook for contract performance and equipment.
* After Installation Site Survey: After WLAN installation, perform a site survey to validate the designed architecture. The goals of this survey are as follows:
  + Verify sufficient Radio Frequency (RF) signal strength and Signal to Noise Ratio (SNR) throughout the coverage area
  + Verify adequate overlap between adjacent WAPs to ensure proper roaming capabilities
  + Measure and reduce Co-channel Interference (CCI) among WAPs operating on the same channels
  + Validate actual client performance for mobile devices used at the post
  + Verify that the Wi-Fi signal does not exceed the CAA signal strength limitation as specified in the current DS WLAN Security Standard for DIN.
* Inspection and Acceptance Criteria: Perform an independent signal attenuation survey (SAS), cable testing, and Wi-Fi coverage analysis that meets the requirements and provide the results to DOS designated representatives.
* Inspection and Acceptance Criteria: The acceptance period for exiting Posts shall be a continuous 30-day period of no system hardware generated major alarms or loss of Wi-Fi service.

### Regional Relay Facility - Network Engineering

* Execute tasks for the installation/de-installation of networking/security devices/systems and associated connections (i.e., fiber/copper jumpers and power cables). Related tasks also include connection labeling (i.e., distribution patch panels, network connections, power cables), communication cabinets/racks modifications, and fitting of related mounting hardware; Installations take place in a variety of areas throughout the telecommunications center and linked workspaces.
* Perform preventive maintenance and/or remediation activities (ex. Jumper cabling termination/repair/correction; periodic testing, rack clean up, etc.) necessary for maintaining the reliability of infrastructure, and resolving issues/failures.
* Conduct documenting of results of testing/verification (ex. circuit/service acceptance, higher tier support service verification, etc.)
* Oversee occasional installations conducted by external agencies within the telecommunications center and conducting quarterly inspections/audits to verify and enforce agency installation standards and industry best practices within the facility.
* Maintain equipment and tools related to installations, testing/analysis, and repair of supporting IT and networking substructure.
* Deliver local system integration support for internal/external end-users (ex. troubleshooting, technical consulting, assistance with system deployments, etc.) deployments/maintenance, etc.) for systems/equipment housed within the TCF.
* Provide Tier 3 IT maintenance support (i.e., H/W upgrades, higher tier maintenance, issue resolution, etc.) for locally managed DOS and OGA core systems.
* Conduct periodic training of new/current on-site support personnel on use of managed support systems and equipment.
* Perform quality checks of deliverables resulting from the completion of customer requests for change/service; Checks consist of inspection of installed equipment, associated infrastructure (i.e., backbone fiber/copper cabling, distribution patch panels, network connection boxes, associated conduit systems, identification labels), accuracy of linked records within databases/folders, and other related documentation.
* Identify defects/errors in deliverables, arranging remedial actions with appropriate personnel, and documenting/reporting on discoveries, remediation, and isolation of root cause(s) in organizational reports and meetings.
* Assist in the implementation and maintenance of quality control policies/procedures; recommending process improvements to mitigate risks and prevent future occurrences of issues to the quality of work products/deliverables.

### Operations Center Support

* Provide Tier II support that includes analysis of all conditions that affect enterprise network and systems availability, reliability, performance, security and resulting recommendations and actions for continuous improvements.
* Provide support for the transition of projects developed by DOS into Operations and Maintenance (O&M), to include development of appropriate documentation establishing operational procedures.

### IT Service Management (ITSM): Tier III Network Support

* Implement a methodology for ensuring the availability of the Department’s networks through continuous monitoring of the global network infrastructures, identifying potential sources of congestion or conflict, and proactively eliminating potential network performance trouble spots.
* Provide Tier III engineering support required for continued expansion and update of OpenNet and ClassNet efforts.
* Proactively identify network performance trouble spots and take steps to fix before network outages occur.
* Provide Tier III engineering support to Operations and DOS posts worldwide, assisting Operations in resolving operational network and system issues.
* Provide 24/7 x 365 support on all DOS networks, re-prioritizing and adding all resources as necessary if directed by senior management. Examples of this include network compromise or attack, or major failure in the routed infrastructure.
* Resolve outstanding network problems relating to circuits, routers, switches, and encryption equipment. The networks include the Department’s OpenNet and ClassNet networks and any other supported networks.
* Work with other DOS IRM operation entities to resolve information technology related problems, including Domain Name Service (DNS) related problems, Department File Transfer Protocol (FTP) server related problems, and Windows Internet Name Service (WINS) related problems.
* Escalate and work with the appropriate vendors to obtain the fix or design a new solution to fix incidents and problems as required.
* Maintain troubleshooting tools necessary to perform Tier III support functions (network protocol analyzers, etc.).
* Perform all Tier III support in accordance with the DOS ITSM processes and using DOS ITSM tools, including the use of the enterprise ticket system and internal change processes for incident tracking and change approval.

### IT Service Management (ITSM): Tier II Network Support

* Operate and maintain an operations center at State Annex – 26 (Beltsville, MD), or wherever designated by the COR, which will support DOS’s global enterprise network and related systems 24 hours per day, 7 days per week, 365 days per year in 24 time zones.
* Provide multiple shifts that meet 24/7 x 365 core support requirements of the enterprise network and related systems.
* Establish effective procedures and control systems to ensure ongoing tasks, unresolved problems, and general issues of concern are properly handed off by the departing shift to the arriving shift.
* Maintain existing staffing, scheduling, and workflow plans (see deliverables)
  + Providing a staffing plan to ensure all task requirements are met with qualified and cleared personnel. The Plan shall be updated by the contractor if required by DOS management
  + Reviewing existing operational workflow plans and providing updates that ensure timely and responsive customer service using existing Department processes. The contractor will deliver these plans to DOS management personnel for review and approval. The contractor will provide a semi-annual review or on an as-needed basis as required by DOS management
* Provide 24/7 x 365 monitoring of DOS unclassified and classified enterprise networks (i.e., core routers and switches, domestic and overseas) and systems (i.e., Windows Domain Controllers and all servers hosting network and systems tools) employing a variety of network and systems software tools (all core systems components transitioned), including several which provide input data to a visual graphic display wall.
* Continuously conduct comprehensive enterprise network and systems analysis, which includes but is not limited to:
  + Immediate identification of failures as identified by on-line tools and the video wall display.
  + Escalation to Tier III within two hours or sooner if the issue is determined to be by its nature Tier III design, project(s) not transitioned to Operations, systemic, or chronic failure, etc.
  + Adherence to established reporting mechanisms: ServiceNow Incident management system, Firewall Advisory Board (FAB), Internal Change Advisory Board (ICAB), and Classified Internal Change Advisory Board (CICAB)
  + Adherence to change management policies as established by DOS’s Technical Review Board (TRB)
* Provide early warning of potential network issues before they impact network availability and monitor server events and performance that could impair the Department’s ability to conduct the Department’s business.
* Evaluate network and systems tools capabilities for continuous improvements and liaise with DOS stakeholders to ensure that the ENMOC’s requirements are formally incorporated in future tools identification, selection, development, and operations.
* Deliver rapid response to real or potential network and systems faults in accordance with established Tier II support and Tier III escalation procedures.
* Provide on-call fault management actions to isolate and resolve problems in accordance with established Tier II support and Tier III escalation procedures.
* Administer the local area network (LAN) hardware and systems (e.g., Operating System, software maintenance).
* Support the operation of the DOS Federal Zero Trust Architecture (ZTA) as required, potentially to include micro-segmentation and software defined networking (SDN), in coordination with the DOS cybersecurity organizations within IRM and DS and potentially with a Zero Trust program office.

### Centrally Monitored and Engineered Security Controls Support

* Operate existing centralized security systems and automated tools to monitor and control security configurations and standards, and to recommend continuous improvements towards realizing an increase of systems and information integrity.
* Centrally monitor DOS networks to provide notice of significant security events to authorized, designated personnel in a timely fashion and through a DOS approved notification method, i.e., DOS’s Incident Handling Process.
* Identify the security vulnerabilities associated with the organization’s systems, applications, and operations and providing recommendations and plans to eliminate them whenever possible and mitigate all others.
* Establish controls to assure compliance with DOS security standards. These configurations are identified in the security standards established by Diplomatic Security guidelines and other documentation.

### Regional Relay Facility Network Service Center - Network Monitoring

* Employ methods or formulas to correlate network activities to service quality/deficiencies.
* Diagnose and isolate Enterprise Network deficiencies to the component level to develop and implement corrective actions tactics.
* Prepare reports depicting quality of service, patterns/trends, and historical data for use in the development of correction action plans, forecasting future needs or similar matters requiring further study or remedial action.
* Assist in the isolation/resolution of Enterprise Network deficiencies; establish temporary routing alternatives.
* Coordinate with customers, Government agencies and commercial vendors the troubleshooting, testing, installation/deletion of new or existing services to meet customer’s communications requirements.
* Ensure that all operational tasking is coordinated and completed within the designated time/priority assigned by Management.
* Document all taskings in the DOS ITSM system of record (e.g., ServiceNow) with clear and concise information.
* Pass all ongoing issues, outages, and tasking during shift change to the oncoming shift with minimal interruption (i.e., relatively unnoticeable to all customers).
* Escalate operational tasking as required to management and Watch Officers (WO) on duty immediately to resolve it in a timely manner.
* Quality check all completed work by someone other than the engineer who completed the tasking and verified by WO on duty before the Task is closed out and forwarded onto Engineering.
* Conduct Viper secure phone tests once a day by one of the Shifts and any issues shall be reported/escalated, as necessary.
* Report Network Core Systems availability.
* Gather and report customer satisfaction surveys.
* Report on service request completion.
* Update, Maintain, and Report on all Incidents and Service Requests assigned to the NSC.
* Ensure Incident (INC) and Service Requests (SRs) are updated at all times including troubleshooting efforts, issues, resolutions, along with any pertinent information.
* Contact customers regarding INC and SRs using every option or tool available to try and reach the customer.
* Report and verify that data network changes were completed on time.
* Verify that GPS systems are operating properly and escalate any issues noted.
* Continually work to maintain ISO20K certification.
* Ensure DCIM environmental systems supporting hosted systems are operating properly; Provide DCIM Technician support for RRF stakeholder owned equipment.
* Monitor Classified Tunnel and report any alarms issues noted.
* Provide Security and COMSEC Support.
* Provide 24/7 x 365 Operational & Maintenance (O&M) support for the Classified Cores and Beltsville Information Management Center (BIMC) and Harry S. Truman (HST) location.
* Provide Local Area Network (LAN) Services to those customers we support within Beltsville Information Management Center (BIMC).
* Provide TACLANE Support for Overseas and Domestic customers.
* Provide support for the State Optical Core (SOC).
* Maintain, operate, and update GEMONE (INE S/W provided by General Dynamics).
* Support IRM Change Advisory Board (ICAB) and provide Change Request (CR) submissions as required.
* Operate NeuralStar maintaining and updating filters when necessary.
* Provide Core Encryption Installations and Maintenance.
* Update and Maintain Power Management.
* Provide GTS Facility Oversite (Secondary Tech Control and adjacent spaces).
* Provide Trusted Internet Connection (TIC) support.
* Be prepared to support facility during fire alarms, emergency situations and for any drills that are conducted.
* Coordination with IT service center, IT service desk, and other service providers, as needed, classify, and prioritize events, incidents, and problems (Critical/High/Medium/Low).

### Capacity Planning for Department Bandwidth Requirements

* Provide recommendations regarding the bandwidth necessary to support the Department's business requirements as specified in the yearly capacity plan using both commercial and government carriers as directed by the Government management team.
* Plan the collection of enterprise application requirements from DOS bureaus and its foreign affairs partners and develop user requirements into circuit bandwidth and performance requirements on an annual basis.
* Perform application bandwidth usage modeling and simulation using commercially available modeling tools and provide both ad hoc and annual bandwidth forecasts to the Department to support its circuit procurement process.

### Quality of Service (QoS) Support

* Actively monitor the Department’s global enterprise network, enterprise applications and their conditions, taking prompt action to improve the quality of the Department’s circuits.
* Provide prompt necessary action and communications to improve or resolve issues which can include but are not limited to:
* Network reliability and availability
* Latency issues
* Asymmetric routing
* Unusual throughput levels
* Downed circuits
* Packet loss
* Network congestion
* Load sharing options
* Identifying candidates for bandwidth increase requests
* Identifying speed and duplex mismatches of the Department’s global enterprise network
* Provide expert ability to analyze network throughput, latency, other key network performance criteria for enterprise network(s) using available and approved monitoring tools.
* Provide objective and actionable recommendations to address findings from continuous monitoring, analysis, tools, etc. across the Enterprise Network(s).
* Facilitate and attend regularly scheduled meetings and provide reporting for Quality of Service meeting and produce DOS Watch list report which includes but is not limited to:
* Weekly availability of poorest performing circuits for which DOS is responsible
* Primary or secondary circuits that are down for a specified amount of time
* Recent packet loss data to various points along all DOS circuits
* Latency and Availability issues to include but not be limited to performance measures of foreign circuits and seat counts from Active Directory
* Collaborate with other teams to optimize performance of distributed applications.
* Communicate with the correct entity (e.g., other Tiger action offices, post personnel, or ISPs) to prompt action on any known issues involving the DOS global enterprise network or enterprise applications.
* Provide management of and act as the FW technical representative of the (Firewall Advisory Board) (FAB).

### Wi-Fi Operations Services

* Warranty, Maintenance & License Support: All material delivered, including spares, shall have a warranty, maintenance, and licensing period for a minimum of three (3) years from acceptance date or per direction of the government.
* Warranty, Maintenance & License Support: Repair or replacement of any item during the warranty and / or maintenance period shall be at no cost to the Government, and the contractor shall provide substitute or replacement equipment during the period of repair. These rights listed below shall be in addition to those provided by FAR 52.246-19 Warranty of Systems and Equipment.
* Warranty, Maintenance & License Support: All of the systems installed by the contractor shall have an operational life of at least ten years, with the exception of the WAPs which will have an operational life of 3-5 years. Provide certification in its proposal that it has reasonable expectation (and the factual basis for that expectation) those parts shall be available for purchase for the systems the Government buys to ensure life cycle support for a minimum of 10 years, beginning on the date of system acceptance.
* Warranty, Maintenance & License Support: Provide a defective parts exchange process whereby:
  + DOS shall obtain a return authorization number by e-mail any weekday between 0730 hours and 1630 hours ET. The plan shall include notification procedures to the COR of Post outages, shipping status of parts, and requests for COR assistance.
  + The contractor is liable for replacement of, and all shipping costs associated with, the replacement part to and from DOS’ Offices at SA-21 or a location within the NCR.
  + During the warranty period, the contractor shall expedite all failed components to arrive at SA-21 or a location within the NCR within five (5) business days of receipt of failed equipment.
* Warranty, Maintenance & License Support: Provide on-call, on-site at SA-21, remote maintenance support for the Wi-Fi enterprise systems on a 24X7X365 basis at a minimum for the first two years of the contract.
* Support remote maintenance to monitor the health of each Post’s Wi-Fi. Currently Wi-Fi goes through a FIPS 140-2 encryptor. Provide immediate, direct support when the Government determines an immediate solution is required (e.g., system down or a majority of the system not functioning).
* Warranty, Maintenance & License Support: Each Post’s Wi-Fi system shall be available 24 hours a day, seven days a week, except for DOS-approved scheduled service interruptions. The inherent availability of the system including all subsystem components shall be at least 99.9994%.
* Warranty, Maintenance & License Support: Provide systems designed for rapid repair using automatic fault location and plug-in modules to the maximum extent practicable. The system shall have a MTTR of not more than 0.5 hours and shall have a total time to repair of not more than one hour for at least 90% of all system faults.
* Shall design all main systems with sufficient redundancy to ensure a system downtime to system/subsystem failure of not more than four hours in twenty years.
* Provide advisory services to DOS of all hardware and software upgrades to the installed systems, as they become available on the commercial market.
* Equipment Installation: Engineer, furnish, pre stage and burn in to identify defective parts before delivery, apply protective technology, asset tag, stage, configure, install, integrate, label, test, and make operational all equipment in the type, quantity, and configuration ordered or provided as GFE, based on technical direction from the COR, and accepted deliverables.
* Equipment Installation: Provide all hardware, supplies, and tools necessary to install, move, program, test, maintain, and repair all equipment delivered.
* Equipment Installation: Ground all power supplies and equipment cabinets it installs, in accordance with the manufacturer's recommendations and with all applicable codes. All work shall conform to accepted telecommunication installation and repair standard practices and the recommended practices of the manufacturers of the equipment and materials used.
* Provide all protective technology, seals, and label all devices that require it.
* De-install and dispose of equipment: De-installation of equipment includes all labor, tools, and incidental parts or material necessary to accomplish equipment removal, including equipment cabling.
* Dispose of the Government –owned equipment, unless otherwise requested.
* Remove all contractor-owned or leased equipment used during the installation as well as all storage and packaging materials.
* Familiarization Session(s): Conduct on-site technical overview and familiarization sessions in a classroom or a "hands-on" environment, using the actual equipment in a full operational mode.
* Familiarization Session(s): Provide the following logistical procedures to the Post IT Systems Management Staff:
  + Replacing equipment items under warranty, from the spare parts inventory and then ordering a replacement item from DOS.
  + Replacing equipment items under warranty not included in the spare parts inventory.
  + Ordering expansion/additional equipment items.
  + Ordering replacement equipment items for maintenance purposes after the warranty period and after task order expiration (i.e., lifecycle support).
* Deliverables: All material produced shall become the property of the U.S. Government. Deliverables shall meet the following principal objectives:
  + Illustrate coverage area of the Wi-Fi signal based on the optimal placement of the WAPs for all customer requested areas
  + Outline the methodology used to conduct the survey at mission location
  + Identify the Wi-Fi equipment and architecture
  + Identify nearby RF signals and potential sources of interference
  + CAA spaces require special attention to ensure AP signal penetration levels do not exceed the requirements specified in the current version of the DS WLAN Security Standard for DIN.

### Contingency Planning Support

* Support DOS efforts to establish and operate (when necessary) an alternate communications facility at the DOS designated site, currently in Washington, DC and Springfield, VA, but potentially to migrate to ESOC West, CTC, or another facility at the DOS direction.
* Maintain DOS alternate communications site to ensure the continuity of the DOS networks in the event operations at the ENMOC (SA-26) are no longer viable because of scheduled or emergency events.
* Provide support for periodic contingency planning exercises conducted by Government or other authorized personnel to ensure the effective implementation of the processes and procedures required to implement the appropriate recovery efforts on behalf of DOS.
* Periodically review the DOS-approved shutdown procedure and recommend changes as appropriate to ensure that systems and network devices are disconnected in the appropriate order in response to an approved emergency. This procedure shall include the processes required to transfer operational control to a designated alternate communications site, and to provide skilled and qualified operational staff to that alternate site as directed in the procedure.
* Periodically, as directed by the Government, exercise the Emergency Shutdown and Recovery Procedures.

## Endpoint Engineering and Support

Endpoint engineering and support are concerned with the development, deployment, sustainment, and retirement of endpoints and the associated operating system for the entire Department. Standard operating environment responsibilities shall include, but are not limited to, managing changes to the environment (e.g., operating systems, applications), lifecycle support for the network as well as security and access management tools, supporting the IT Change Control board process and defining/refining processes as needed. The following table identifies the roles and responsibilities.

### Endpoint Engineering and Design

* Define high level standard operating environment strategies, service requirements, and policies.
* Test, pilot and follow the change management process for approved Standard Operating Environment (SOE) for servers and workstations software.
* Engage application owners, testers, and developers while following standard software lifecycle practices.
* Provide quality operation system builds that assist customers in meeting their mission.
* Engage with high level technical and engineering representatives, as well as other representatives from a variety of offices within DOS to automate and streamline change management processes in support of the SOE.
* Define the structured lifecycle of approved Operating Systems (OS), their interaction with approved applications and the maintenance of an adequate IT security posture throughout the Department.
* Analyze existing policies and processes to propose sound modifications to Evolve those policies and processes as appropriate to ensure efficient, effective, and timely integration of new OS’s, applications, and security configurations, leading to the implementation and maintenance of a SOE.
* Provide administrative and management support for matters pertaining to enterprise-wide SOE management, security guidance and policies.
* Identify and document software release management and delivery incorporating the approved comprehensive and scalable solution for the change control board; and help achieve a standard operating environment configuration.

### Enterprise Software Packaging and Distribution (ESPD)

* Perform high level integration, functional, regression and acceptance testing on applications for the Standard Operating Environment (SOE) core desktop, laptops, workstations, and servers.
* Create operational builds based on approved hardware, software, and Diplomatic Security configuration standards for use for the enterprise.
* Develop, manage, and maintain the Department’s state-of-the-art IT “Underwriters Lab (UL)-type” laboratory, helping to lead a global standardization effort and provide added assurance of quality and integration to any product that is tested in the facility.

### Patch Management Support

* Support enterprise-wide Patch Management program and lab through
  + Collaborations with the DOS architects of the overarching infrastructure
  + Establishing approved, comprehensive, and scalable solution(s) to discover, assess, test, package, distribute, troubleshoot, and validate security bulletins for the DOS network environments
  + Attaining and maintaining a successful patch state that ensures all applicable patches are applied in a timely manner
* Administer and facilitate the application of required patches enterprise-wide and provide remote, centralized engineering support to customers.
* Incorporate and communicate relevant government policies and procedures relating to enterprise-wide patch management functions.
* Stay abreast of emerging patch management trends and technology, provide recommendations to management, and implement approved technologies as appropriate.
* Coordinate activities with patch management stakeholders and customers, to ensure consistent patch management processes are understood throughout DOS.
* Provide 24/7 x 365 on-call standby Patch Management support in accordance with the DOS ITSM processes, whereby points of contact are available for follow-up actions regarding critical patch events.
* Develop, maintain, and update patch management website(s) to keep the DOS enterprise informed of the program, and provide timely information and updates on patch activities and distributions.
* Maintain DOS’ state-of-the-art lab and lab processes in which to perform installation, regression and interoperability and deployment testing of patches on appropriate Operating Systems, applications, and hardware components.
* Develop, implement, and support, in a collaborative and matrixed manner, a centralized software distribution method in support of new/updated applications or security fixes, certain core applications and Operating Systems to client workstations and servers throughout the enterprise, which will also serve to facilitate a standard operating environment throughout the DOS.

### Systems Management Support (Microsoft’s Endpoint Configuration Manager (MECM))

* Maintain the DOS on-premises centralized System Center Configuration Manager (SCCM) infrastructure v 1909 or later versions if upgrades of infrastructure occur.
* Maintain, recover, troubleshoot, upgrade, patch and monitor the core infrastructure hardware and software.
* Initiate change requests and follow established change management procedures.
* Perform the design, setup, engineering, management, deployment, improvement, documentation, and implementation of changes to core MECM infrastructure for OpenNet, ClassNet, and other DOS supported networks.
* Perform the design, setup, engineering, management, deployment, improvement documentation and implementation of changes to the core Intune environment in Microsoft Cloud.
* Identify, evaluate, research, test, deploy and implement cost-effective tools that assist in managing DOS global enterprise MECM infrastructure.
* Document the processes and procedures for system users/administrators utilizing the MECM system.
* Work with the Patch Management Team, iPost Team, or any other designated group for reporting and implementation of system patching throughout the Department’s global enterprise.
* Ensure all MECM packages reach all distribution points throughout the enterprise.
* Work with the Patch Management Team to push patch packages to all distribution points throughout the enterprise and provide updates, status, and reports upon request.
* Install all necessary tools to all MECM clients in the enterprise (domain controllers, application servers, and other identified servers can be excluded unless the appropriate agreement is made with the proper authority and approval).
* Troubleshoot, coordinate, and resolve all MECM client issues.
* Keep post and site administrators informed through reports and communication of their sites’ status.
* Work with iPost and Discovery Teams to ensure that all data is valid and being reported accurately.
* Review, update, amend, draft, negotiate, and gain initial and final approval for all documentation to include, but not be limited to SLA’s, Standard Operating Procedures (SOP), guides and manuals.
* Create, maintain, and update knowledge-based articles, help files or FAQ’s that provide information, explain functionality, or resolve issues for users and other stakeholders.
* Conduct testing of any changes to tools or enhancements prior to being implemented into a production environment.
* Serve as knowledge expertise in regard to confidentiality, integrity and availability for the Department on MECM and working closely with appropriate personnel or offices (e.g., working with Diplomatic Security on developing security configuration guides and security templates).
* Provide operations and maintenance at all Tier levels for any issues dealing with the MECM infrastructure.
* Provide access to tools for managing MECM sites to users/administrators.
* Ensure the availability, functionality, upgrades, performance of tools used by MECM Team and users.
* Provide secure approved mechanism for users to request proper approval and access to MECM tools.
* Provide support Post Administration Tool (PAT).
* Ensure system or tools, if deemed necessary, obtain Security Accreditation and Authorization (A&A), and once obtained to ensure that the status remains up to date.

### Compliance

* Plan the transition of DOS networks to Ipv6 and any other future mandates provided by the OMB, as well as other applicable regulatory bodies.
* Assist with all aspects of planning and transitioning DOS networks to Ipv6 and any other future mandates provided by the OMB, as well as other applicable regulatory bodies.

### Lifecycle Support

* Manage the network life cycle on a proactive basis, providing new connectivity solutions and technology refreshments, taking into consideration: maintenance costs, technology obsolescence, new user requirements, and cost per bit of data transmitted.
* Develop a five-year predictive spend plan to replace hardware equipment in alignment with vendor End of Life (EOL) / End of Support (EOS) plans.
* Provide lifecycle support of IT security and access management tools for the Department’s Unclassified, Classified and Cloud networks and systems.
* Assist DOS in sustaining a secure enterprise network by maintaining, testing, and controlling changes in the IT Standard Operating Environment (SOE) and a core set of IT CCB Baseline products in a managed Lab environment.
* Mitigate software and hardware security vulnerabilities by providing patch solutions, supporting automated distribution methods for a core set of products, supporting applications packaging and IT request, as necessary.

## Customer Facing Services

Customer facing services provide direct liaison with a variety of customers, internal primarily but also external. Customer facing services must always maintain a high level of professionalism and customer-first service management.

### 24/7 x 365 IT Operations Center Support (ITOC)

* Operate and maintain an Operations Center at State Annex – 9 (Washington, DC), or wherever designated by the COR, which will support DOS enterprise IT Operations Center and related systems 24 hours per day, 7 days per week, 365 days per year in 24 time zones.
* Provide multiple shifts that meet 24/7 x365 core support requirements for the ITOC.
* Establish effective procedures and control systems to ensure ongoing tasks, unresolved problems, and general issues of concern are properly handed off by the departing shift to the arriving shift.
* Review existing operational workflow plans and provide updates that ensure timely and responsive customer service using existing DOS processes. Deliver these plans to DOS management for review and approval. SLA requirements for timely and responsive customer service.
* Provide reviews of operational workflow plans on a semi-annual or as-needed basis as required by DOS management.
* Maintain a list of all critical Missions/sites and services.
* Provide 24/7 x 365 monitoring and support for all critical Missions/sites and services.
* Identify, manage, and support all high severity (SEV) service impacting issues across the enterprise.
* Coordinate issue resolution by hosting and facilitating conference calls and other communications with technical subject matter experts, engineers, vendors, and other IT support staff.
* Facilitate and publish After Action Reviews (AAR), and Situational Awareness Report for all SEV-1 and SEV-2 incidents.
* Rapidly respond to real or potential network and systems faults, providing on-call fault management actions to isolate and resolve problems, in accordance with established Tier II support and Tier III escalation procedures.
* Provide input for strategic, tactical, and project planning.
* Support DOS Earned Value Management System (EVMS).
* Perform technical writing, documentation, and version control.
* Manage electronic file folders and directories
* Provide status reports as requested by DOS, to include preparation of activities for the Weekly Achievement Report (WAR).
* Track project time expenditures for all Network Services contractor personnel.
* Provide highly skilled personnel, during all ENMOC shifts, which possess the same high level of network/systems expertise and capability to effectively support global operations 24/7 x 365. Formal systems engineering degrees and industry standard certifications are considered an advantage and indicator of ability to successfully conduct the business of the ENMOC.
* Provide qualified and knowledgeable contract personnel that are sufficiently capable in the practice of customer relations in order to provide our customers domestic and abroad the best possible support experience.
* Provide trained and qualified personnel to conduct daily operations of all network and system toolsets to include: NeuralStar, Splunk, Cyber Ark, HPNA, Wireshark, PANORAMA and other toolsets deemed necessary by DOS.
* Provide qualified and knowledgeable contract personnel that are sufficiently capable in the practice of customer relations in order to provide our customers domestic and abroad the best possible support experience.
* Ensure that contractor labor charges are reported accurately and coordinated with the DOS Planning Staff for the purpose of developing Earned Value Management System (EVMS) calculations.
* Create, maintain, and update knowledge-based articles, help files or Frequently Asked Questions (FAQs) that provide information, explain functionality, or resolve issues for users and other stakeholders.
* Cooperating and coordinating with DOS Information Systems Security Officer (ISSO) to assure all contractor personnel successfully complete mandatory annual computer security awareness and other related requirements as identified by Department authorities.
* Perform and comply with all security, configuration, and other documented processes as required.

### Regional Relay Facility Network Service Center (NSC)

* Provide 24/7 x 365 support to the Network Service Center (NSC) by monitoring, managing, and maintaining core enterprise network devices and core system components within Department of State (DOS) unclassified and classified networks.
* Maintain service and system documentation and knowledge base materials along with following and participating in standard ITIL best practices and International Organization for Standardization 20000 (ISO20K) certifications to maintain the services.
* Always provide two-person integrity (TPI) to manage the system of storage and handling designed to prohibit individual access to certain COMSEC keying material by requiring the presence of at least two authorized/cleared individuals, each capable of detecting incorrect or unauthorized security procedures with respect to the task being performed.

### IT Change Control Board (ITCCB) Support

* Perform analyses and provide recommendations to the IT CCB management staff of all proposed systems, components, and changes to the IT CCB baseline, ensuring that all meet DOS accepted standards.
* Manage IT systems changes that impact the DOS global IT environment, in a planned, systematic, and timely manner, using Configuration Management best practices.
* Provide administrative and management support to the IT CCB Chair and IT CCB Change Manager for matters pertaining to enterprise-wide change management and IT CCB proceedings, and appropriate subgroups.
* Incorporate the approved comprehensive and scalable solution for the change control board.
* Make recommendations for process improvement and help achieve a standard operating environment.
* Provide administrative and management support to the IT CCB Chair and IT CCB Change Manager for matters pertaining to enterprise-wide change management and IT CCB proceedings, and appropriate subgroups.
* Assist and participate in developing, implementing, updating, and maintaining Standard Operating Procedures, policies, training materials and briefings, internal process flowcharts, forms, annotated agendas, meeting minutes, baselines, websites, general communications, and reports as they relate to management and support of the IT CCB and its objectives.
* Audit and evaluate IT CCB and Local Change Requests for scope, risk, and duplication. Report findings and provide recommendations on an annual basis or more frequently if needed.
* Maintain the DOS baselines for the IT CCB in a timely manner and specify components of the DOS baselines by name, function, sub-components, ownership, and other pertinent items as appropriate. Draft any new baselines as directed.
* Provide routine and/or ad hoc reports on the DOS baselines as requested.
* Review and communicate relevant policies, and consult with DOS technical experts as appropriate, to provide recommendations to the IT CCB Change Manager and guidance to customers regarding:
  + Phase 1: Additions, changes, or deletions to infrastructure components (hardware, software, enterprise network devices, firewalls, cabling, wireless, documentation, and settings)
  + Phase 2: Changes to or termination of applications and systems that could affect the performance, security, integrity, reliability, availability, or interoperability of the global infrastructure and/or existing applications
* Conduct quality scope reviews of Change Requests to determine affected baseline(s), whether additional information is required, and for redundancy.
* Coordinate with the Change Manager for all agreed-upon CCB process milestones and timeframes.
* Prepare IT CCB meeting agendas and minutes.
* Facilitate IT CCB and IT CCB subgroup meetings, conduct and validate voting results, and notify DOS of approved changes.
* Measure and track work products, deliverables, and communications, and produce management reports as required.
* Assist in establishing and then implementing an automated IT CCB process which can tie into other DOS processes and databases to the fullest extent, as directed.
* Collaborate with other offices/entities within DOS and other government agencies as directed to collaborate, automate, and streamline change management processes.

## Radio Communications

Radio communications are concerned with the engineering, development, deployment, sustainment, and retirement of land mobile radio systems as well as other associated technologies.

### Distributed Antenna System (DAS)

* DAS equipment and services provided shall be equal to or better than the DAS commonly used in business applications in quality, design, construction, and performance. All DAS equipment and services shall meet the following criteria:
  + Must be an approved enterprise solution
  + The solution shall meet federal, DOS, and local policy, standards, and guidelines.
  + The endpoint cannot be controlled by the service provider and shall be maintained by cleared Americans
* Warranty, Maintenance & License Support: Provide a defective parts exchange process whereby:
  + The contractor is liable for replacement of, and all shipping costs associated with, the replacement part to and from site.
  + During the warranty period, the contractor shall expedite all failed components to arrive at site within five (5) business days of receipt of failed equipment.
* Conduct planning and engineering to ensure DAS signal does not exceed the CAA signal strength limitation as specified in the current DS WLAN Security Standard for DIN and / or appropriate policies.
* Provide an After Installation Survey after the DAS installation to validate the designed architecture. The goal of this survey is to verify that the DAS signal does not exceed the CAA signal strength limitation as specified in the current DS WLAN Security Standard for DIN.
* Survey Report: Meet the principal objectives of the Survey Report:
  + Illustrate coverage area of the signal based on the optimal placement of the equipment for all customer requested areas
  + Outline the methodology used to conduct the survey at mission location
  + Identify the DAS equipment and architecture
  + Identify nearby signals and potential sources of interference
  + Note: CAA spaces require special attention to ensure signal penetration levels do not exceed the requirements specified in the current version of the DS WLAN Security Standard for DIN.
  + Warranty, Maintenance & License Support: Provide on-call maintenance support for DAS.

## Network & System Tools

Network and systems tools responsibilities shall include, but are not limited to, providing oversight, lifecycle support and operations and maintenance for tools (e.g., monitoring, configuration, administration, security, access management) used to ensure network availability and security. The following table identifies the roles and responsibilities.

### Security and Access Management Engineering

* Maintain and provide oversight of tools that grant authorized users the rights to network systems and prevent access to non-authorized users.
* Provide lifecycle and Operations and Management (O&M) support of Information Technology (IT) security and access management tools for the Department’s Unclassified, Classified and Cloud networks and systems.
* Support robust tools to manage, configure and monitor the Department’s global enterprise security and access to devices.
* Identify, evaluate, research, test, deploy and implement cost-effective, scalable, and robust security and access management tools that provide monitoring, performance management, fault management, configuration management incident management, patch management and security management for DOS global enterprise network and systems devices.
* Upgrade tools based on evolving requirements.
* Provide expert knowledge of tool(s) capabilities and functionality.

### Common Network & System Tools Requirements

* Provide network design and engineering efforts to meet the DOS network reliability and availability objectives, including investigating and implementing network management tools to monitor the health of the network and incorporating redundant network design features to minimize outages.
* Provide expert knowledge of existing monitoring tools capabilities and their functionality for use in providing necessary monitoring. Tools are, but not limited to: CiscoWorks (Campus Manager), Cisco Secure ACS, Tavve, HP OpenView, NetVCR, NIKSUN NetX, NeuralStar, RSA SecurID, Marconi’s Service on Data, SmokePing, RedSeal, DS-RADAR, HPNA, Service Now, and Various Reporting Tools.
* Maintain and provide oversight of tools that provide enterprise-wide administration of the Department’s system networks.
* Provide lifecycle and Operations and Management (O&M) support of Information Technology (IT) management tools for the Department’s Unclassified, Classified and Cloud networks and systems.
* Review and analyze DOS global enterprise network infrastructure footprint and operational requirements.
* Support robust tools to manage, configure and monitor DOS global enterprise network and system devices.
* Identify, evaluate, research, test, deploy and implement cost-effective, scalable, and robust network and application tools that provide monitoring, performance management, fault management, configuration management incident management, patch management and security management for DOS global enterprise network and systems devices.
* Manage the maintenance, accessibility, recovery, troubleshooting, upgrading, patching, licensing, and monitoring of hardware and software for all the following tools and any future tools: NeuralStar, LiveAction (Netflow), SolarWinds, NIKSUN (NetVCR), CyberArk, RSA SecurID, Cisco Smart Software Manager (CSSM), Cisco Identity Service Engine (ISE), Microfocus Network Automation (MFNA), SmokePing, ServiceNow Configuration Management Database (CMDB), ServiceNow Change Management, ServiceNow Incident Management, ServiceNow Discovery, Splunk, NetIQ Security Manager, Change Auditor, and Systems Center Operations Manager (SCOM).
* Manage the installation, configuration, engineering, management, deployment, improvement, documentation, and implementation for changes to tools.
* Provide a secure approved mechanism for users to request proper approval and access to monitoring tools.
* Maintain confidentiality, integrity and availability of tools and its data.
* Upgrade tools based on evolving requirements.
* Provide expert knowledge of tool(s) capabilities and functionality.
* Manage a central location for access to tools (e.g., intranet/internet page with hyperlink to access each tool)—currently located at intranet webpage Enterprise Management System (sharepoint.com)
* Provide operation and maintenance support as well as resolving reported problems or inquiries for all tools.
* Initiate change requests and following established change management procedures.
* Review, update, amend, draft, negotiate and gain initial and final approval for all new SLAs with the appropriate parties.

### iPost Support

* Support the DOS iPost system to provide a single source for users to monitor aspects of their post or site’s IT Infrastructure to determine compliance with the SOE by aggregating data from Enterprise level tools currently in use (to include iPost-C once deployed).
* Plan and implement lifecycle replacement and maintenance of iPost.
* Perform recovery and monitoring of the iPost.
* Design, implement, manage, and improve iPost.
* Address customer issues related directly or within the scope iPost.
* Maintain high availability and quality of the iPost system to users, to exclude brief, pre-approved scheduled maintenance.
* Communicate scheduled outages to the iPost user community with sufficient prior notice (e.g., communication mechanism—informing the Tier I (IRM IT Service Center) requesting a Scheduled Outage Notification by distributed to their domestic and overseas distribution.
* Control access and privileges of users to iPost.
* Validate integrity of all data output of iPost.

## Directory Services

Directory Services focuses on engineering and operations for the Department’s Active Directory from currently Microsoft and Identity services from currently Okta.

### Directory Engineering Support

* Define Directory Engineering requirements and policies including requirements to support the broader ICAM strategy.
* Design, engineer and maintain secure enterprise-wide solutions for Active Directory, server operating systems and client operating systems.
* Provide integration and implementation of monitoring tools, testing and approval of hot fixes, service packs and Tier III 24/7 support for Windows related issues.
* Maintain, upgrade, patch, recover, troubleshoot, improve, and monitor core enterprise infrastructure hardware device and software for, but not limited to, OpenNet, ClassNet and Cloud hosted system.
* Perform all Active Directory setup, design, engineering, management, improvement, and changes to the infrastructure for, but not limited to, OpenNet, ClassNet and Cloud Hosted systems.
* Identify, evaluate, research, test, deploy and implement cost-effective tools that assist in managing the Department’s global enterprise Active Directory infrastructure.
* Develop and gain approval to adopt a contingency plan for the existing directory infrastructure and to modify if changes are needed or requested.
* Provide Active Directory support and build design for server and client operating systems.
* Develop security templates for appropriate server and client operating systems following DS Security Configuration Guidelines.
* Provide Tier III 24/7 x 365 support for Active Directory, server, and client operating system issues
* Initiate change requests and following established change management procedures.
* Assist and perform design, engineering and implementation of customer domains and infrastructure.
* Design, engineer, improve, and implement security, confidentiality, integrity, and availability, of active directory, server systems, client systems, privileges, administrative accounts in accordance with (IAW) or to exceed existing procedures and policies, which are established by the Department, the Bureau of Diplomatic Security (DS), the Bureau of Information Resource Management (IRM) and DOS. NIST documented best practices can also be considered.
* Serve as knowledge experts in regard to confidentiality, integrity and availability for the Department on Active Directory, servers and clients working closely with appropriate personnel or offices on developing security configuration guides and security templates.
* Ensure the availability, functionality, upgrades, and performance of tools used by Directory Engineering and Systems Team and users.
* Ensure system or tools, if deemed necessary, obtain Security Accreditation and Authorization (A&A). Once obtained, ensure the status remains up to date.
* Provide technical liaison and outreach to stakeholders and other operational entities.
* Provide training, briefings, and demonstrations upon request.
* Manage a central location for access to tools (e.g., intranet/internet page with hyperlink to Access each tool).
* Manage the DOS IP Addressing and Domain Name Service (DNS) (e.g., managing and allocating IP addresses).
* Note: Requires use of a commercially available software tool (currently using EasyIP) to manage the allocation of IP addresses.
* Manage the Department’s DNS infrastructure by maintaining the DNS state.gov and state SBU architectures and the support of infrastructure DNS servers.

## Telecommunications Services

Telecommunication services provide highly available, scalable, reliable, cost effective and secure voice, wireless, radio, antenna systems and telecommunications infrastructure in a multi-vendor environment with integrated turnkey solutions to support diplomatic missions across the world. Responsibilities include common requirements spanning areas such as site surveys, provisioning, maintenance, equipment disposal and many others. Additionally, responsibilities cover telephone, wireless, antenna systems, radio, infrastructure, and telecommunications engineering, solutions, systems, and services.

### Common Requirements

* Adhere to the following constraints and guidelines for acquiring, provisioning, operating, administering, and maintaining required equipment:
  + COTS - All equipment shall be COTS items requiring no further development and shall have been fully tested or demonstrated in the commercial or government marketplace, unless otherwise specified by the government in advance.
  + Network Compatibility - Ensure that telecommunication equipment and CPE is compatible with the existing GFE, networks and infrastructure.
  + Integration – All equipment and services shall be integrated and coordinated with DOS telecommunication projects, processes, networks, and infrastructure and look for efficiencies.
  + Code Compliance - All work shall comply with all applicable national and local codes.
  + Section 508 Compliance – All products provided by the contractor shall comply with Section 508 of the Rehabilitation Act of 1973, as amended.
* All contractor-procured or provided equipment must meet DOS requirements for suitability in seismic areas, according to the DOS OBO seismicity chart.
* All equipment and services shall be integrated and coordinated with DOS telecommunication projects, processes, networks, and infrastructure and look for efficiencies.
* Remote Maintenance Support: Provide on-call remote maintenance support on a 24X7X365 basis.
* Remote maintenance is used to monitor the health systems. Utilize a Federal Information Processing Standard (FIPS 140-2) encryptor for remote maintenance.
* Provide immediate, direct support under circumstances when the Government determines an immediate solution is required, such as a system down or a majority of the system not functioning.
* Provide support to ensure Post’s systems (e.g., phones, telecom, WIFI, Distributed Antenna System (DAS)) are available 24 hours a day, seven days a week, except for DOS-approved scheduled service interruptions.
* Note: The inherent availability of the system including all subsystem components shall be at least 99.9994%.
* Provide systems designed for rapid repair using automatic fault location and plug-in modules to the maximum extent practicable.
* The equipment design and construction shall easily enable maintenance within the specified time constraints. The maintainability and reliability of the equipment shall minimize the need for auxiliary test equipment.
* Note: The system shall have a Mean-Time-to-Repair (MTTR) of not more than 0.5 hours and shall have a total time to repair of not more than one hour for at least 90% of all system faults. DOS measures repair time from the initial indication of a system fault to the time when the fault condition is absent.
* Design all main systems with high availability and disaster recovery as a core principle.
* Site Surveys: Provide access to perform the site (foreign post or domestic) survey and an on-site Government representative during the survey.
* Site Surveys: Perform site surveys, inquiries, and support other interactions (i.e., Local Exchange Carriers- LEC) required to obtain site-specific information needed. Upon completion of the site survey activities, submit for review and acceptance:
  + Post Requirement Survey (PRS)
  + Site Survey Report (SSR)
  + Note: Site Surveys should result in sufficient information to engineer a complete turnkey solution or systems to satisfy the site’s and/or additional requirements set forth by DOS.
* Site Surveys: Provide the specifications, guidance and acceptance criteria required for the development of the PRS, SSR and other related activities.
* Site Surveys: Site activities (as is applicable) can include but are not limited to:
  + In Brief
  + Out Brief
  + Development of PRS
  + Site Preparation (e.g., Heating, Ventilation, and Air Conditioning (HVAC) enhancements, Electrical enhancements, Lightning Protection, Minor facility construction, Security enhancements, Penetrations, Telecommunication Infrastructure)
  + Intermediate Distribution Frame (IDF) Analysis, with DS approved solution as is applicable
  + Cable and alarm the IDF per standards (e.g., ESO and DS)
  + GSM Gateway Analysis
  + Cell Phone Usage Analysis (e.g., phone-to-cell phone calls vs. landline calls cost, post need for cell phone system, Single In-line Memory Modules (SIMM) Analysis, number of cell phone trunks needed)
  + Voice over IP Analysis (e.g., VoIP trunking between the embassy and satellite locations and consulates, circuit designator and bandwidth, other foreign affairs agencies are or will be co-located within the U.S. mission)
  + Station planning and engineering (follow at minimum DOS guidelines)
  + Cable Routing (e.g., cables that depart a CAA going out into a Non-CAA, as well as Cables that depart a CAA transit a Non-CAA and then re-enter a CAA shall meet all DOS security, safety, and operational requirements)
  + Engineering Study
* Scalability & Growth Analysis: Design the equipment and system for growth without the installation of additional equipment, shelves, or cabinets as determined by the site requirement. The installed hardware shall include a vacant slot capacity of minimum 10% for future use and minimum 10% on-site assignable growth spares.
* Note: To the extent possible, parts shall be interchangeable.
* Provide advisory services to DOS of all hardware and software upgrades to the installed systems, as they become available on the commercial market.
* Interoperability: Design and implement systems that are interoperable.
* Incorporate lightning protection into the system(s) to prevent equipment damage caused by transients conducted into the equipment through power or communications lines after being induced onto the line by man-made sources such as heavy switching transients or by natural phenomenon such as lightning transients.
* Make maximum use of protective devices to shunt transients to ground without causing failure of equipment or the protective device.
* Ensure the system provides protection against pulses having the following characteristics:
* Engineer, furnish, asset tag, stage, configure, install, integrate, label, test, and make operational all equipment in the type, quantity, and configuration ordered or provided as Government Furnished Equipment (GFE).
* Provide all hardware, supplies, and tools necessary to install, move, program, test, maintain, and repair all equipment delivered.
* Ground all power supplies and equipment cabinets it installs, in accordance with the manufacturer's recommendations and with all applicable codes. All work shall conform to accepted telephone installation and repair standard practices and the recommended practices of the manufacturers of the equipment and materials used.
* De-install and dispose of equipment: De-installation of equipment includes all labor, tools, and incidental parts or material necessary to accomplish equipment removal, including equipment cabling.
* Dispose of the Government –owned equipment, unless otherwise requested.
* Remove all contractor-owned or leased equipment used during the installation as well as all storage and packaging materials.
* Familiarization Session(s): Conduct on-site technical overview and familiarization sessions in a classroom or a "hands-on" environment, using the actual equipment in a full operational mode.
* Familiarization Session(s): Provide familiarization sessions for logistical procedures identified personnel from prior to cutover. Familiarize these individuals on performing the following tasks, and procedures for carrying out those tasks upon acceptance of the system:
  + Replacing equipment items under warranty, from the spare parts inventory and then ordering a replacement item.
  + Replacing equipment items under warranty not included in the spare parts inventory.
  + Ordering expansion/additional equipment items.
* Ordering replacement equipment items for maintenance purposes after the warranty period and after task order expiration (i.e., lifecycle support).
* Familiarization Session(s): Make available hands-on or Computer-based training (CBT) training at the contractor or manufacturer’s training facility on all phases/aspects of equipment delivered, including system’s concepts, functions, operation, and maintenance.
* Upon completion of the training, certify in writing that the trainees are appropriately trained to maintain all equipment during warranty periods without impact to the warranty provisions.
* Familiarization Session(s): Trained Technicians shall be authorized by the warrantor to examine and repair the equipment without impact to the warranty provisions
* Inspection and Acceptance Criteria: Acceptance shall occur after a full inspection of the solution in accordance with the system acceptance and Statement of Verification and Testing (SOVT).
* Inspection and Acceptance Criteria: The CO and delegated representative (COR) have the authority to inspect and accept or reject all supplies and services delivered.
* Inspection and Acceptance Criteria: Responsible for corrective actions after the initial installation up until 30 days after the system acceptance and SOVT.
* Documentation: The following minimum documentation will be provided to recipients identified by DOS:
  + A signed copy of the system acceptance and SOVT
  + Maintenance and operator manuals
  + Applicable technical documentation
  + A copy of the red line drawings on-site following the cutover of the system
  + As-Built drawings
  + Note: Drawings and other tailored specifications will be treated as Sensitive but Unclassified (SBU). These documents shall be stored in the designated equipment room and shall become the property of the government
* Conduct an on-site visit one month after Site Acceptance and SOVT on projects to evaluate system performance, resolve any issues identified, train, and develop a Follow up Visit Report (FVR).
* Within two weeks (including travel) complete the IFV. Upon completion of the IFV, provide the FVR to the CO and COR as part of the Post Installation Review (PIR).
* Deliverables: All material produced shall become the property of the U.S. Government. Deliverables include but are not limited to:
  + Engineering Study
  + Site Survey Report (Includes the PRS, Draft Site Survey Report (DSSR) and the Final Site Survey Report (FSSR)
  + Communications (e.g., Briefings, Deep Dives, Cables, Incident Reporting)
  + Post Installation Report (PIR)
* Provide information regarding requirements at a specific site, where available and when requested, which may include:
  + NEC, NCC, NOX, LFO etc. or other drawing packages from OBO/Post/LWS
  + The number of buildings, number of employees in each building and physical proximity of the buildings to each other
  + Post questionnaire
  + Counterintelligence Working Group (CIWG) approval
  + IoT requirements
  + Expected amount of utilization at one time
  + Expected mission (Post) telecommunications requirement growth within 5 years
  + Historical resources
* DOS, IRM, and DS polices, standards, and guidelines
* Warranty & Maintenance: Provide the following minimum warranty on products from the acceptance date or per the direction of the COR:
  + A minimum warranty of 20 years under normal conditions
  + A minimum of three (3) years from acceptance date or per direction of the COR for all other material delivered such as electronic equipment, racks, in support of Distributed Antenna System (DAS), etc. under this task order, including spares
* Warranty & Maintenance: Repair or replace any item during the warranty period at no cost to the Government and provide substitute or replacement equipment during the period of repair.
* Warranty & Maintenance: All components and equipment of all of the systems installed shall have an operational life of at least eight years.
* Provide certification in its proposal that it has reasonable expectation (and the factual basis for that expectation) that parts shall be available for purchase for the systems the Government buys to ensure life cycle support for a minimum of 10 years, beginning on the date of system acceptance.

### Telephone / Telecommunications Engineering, Solutions, Systems, and Services

* Ensure that all PBX equipment and customer premise equipment (CPE) is compatible with the existing Government Furnished Equipment (GFE), networks and infrastructure.
* All telephone instruments shall meet the following criteria:
  + The ringer shall have a manual volume control accessible without removing the housing.
  + The contractor shall provide a list of customary colors. The contractor’s customary colors for the telephone instruments shall be available at no added cost.
  + Each telephone instrument shall include a minimum six -foot terminated base cord.
  + Telephone sets shall conform to Bell System Dual Tone Multi-Frequency (DTMF) design parameters and the Electronic Industries Alliance (EIA 470) standard. (Voice over IP (VoIP) handsets are not required to conform to the EIA 470 standard).
* Provide telephone security equipment evaluated and approved for security effectiveness.
* Use of the items on the approved list is a DOS requirement that provides telephone on-hook audio security to CAAs.
* Fax, Modem, Elevators: Provide programmed analog ports and provide service to FAX machines, modems, and elevators.
* PBX/Call Servers: Provide PBXs that support the basic capabilities and system features listed below. PBXs shall meet the Post customer’s requirements, have a digital or analog interface that is compatible with the Local Exchange Carrier’s (LEC) trunk service, and comply with applicable commercial standards and practices.
* PBX/Call Servers: The following features are the minimum required for DOS PBXs:
* All cable to the desktop must be Category (CAT) 6 or better.
* Analog Data Terminal Equipment (DTE) support to connect user provided data communications equipment (DCE) to the system - Analog DTE support shall provide interfacing for user provided DCE and shall be compliant with standard RJ-11, RJ-41, and RJ-45 modular plugs.
* Uniform Call Distribution (UCD) – Spread incoming calls over a group of trunk lines or stations to ensure that all lines or stations carry uniform traffic loads.
* Direct Inward Dial (DID) -The system shall capture, via the trunk circuit, the incoming digits on trunks allowing the caller to reach extensions directly without attendant intervention or assistance.
* Automatic Station Release - Off-hook stations that are idle for 15 seconds shall have the dial tone removed.
* Class of Service and Automatic Station Restrictions – Provide at least 15 groupings programmable to the stations.
* Direct Outward Dial (DOD) support.
* Divert Intercept Treatment Calls – Divert calls to nonexistent numbers to the console operator, information answering position, or intercept recorder, where appropriate.
* Speed Dialing - Intercom type service by dialing one, two, or three digits for frequently called numbers.
* Night Service (Flexible) - The system shall be flexible to allow changes made at the attendant console or management terminal to designate particular stations to receive incoming calls after hours. Selected numbers shall have nighttime incoming calls routed to pre-designated station(s). Activation of this type of transfer shall have a visual indication at the station, which initiates the transfer. The system shall allow incoming calls to activate a night bell for answer by any station after dialing the night answer code. The system shall interface with telephone answering/recording devices (FPT uses a Viking K-600F, which is installed in Post One’s SelecTone system via an analog port off the PBX).
* System Failure Transfer - The system(s) shall provide fail-safe-service, in the event of system failure, from the LEC (connection and dialing) to pre-selected users.
* Trunk Queuing/Call Back On and off hook queuing for outgoing trunk facilities that provides a tone back to the user indicating that the user is in queue, shall be provided. In addition, the system shall call back the user to set up the call when a trunk becomes free.
* Maintenance Diagnostic Subsystem - The application software shall be equipped to monitor the operating condition of the telephone system(s).
* Teleconferencing - The system shall provide multi-party, user originated and controlled (up to six parties), teleconferencing with a mix of trunks and stations.
* Call Tracing - The system shall provide call tracing (station-to-trunk, trunk-to-station, and trunk-to-trunk) and malicious call tracing for trouble shooting purposes.
* Traffic and Usage Data - The systems shall provide automatically recorded traffic data on originating, terminating intra-system (station to station) and trunk and circuit usage. Systems of 51 ports and over shall provide at a minimum:
* Number of calls
* Call duration
* Calls per station during peak hour
* Number of occurrences of all facilities/trunks busy and overflow for each operational access code
* Number of stations dial tone delays of more than three seconds
* Traffic load carried for each trunk group
* Average busy hour answering time per console group
* Number and percentage of calls exceeding 20 seconds answer during the busy hour
* Average and maximum number of seconds that a call is in the attendant queue
* Busy hour load per console position
* Line Release - The system shall lock out the affected line if the calling or called party fails to go on hook. The system shall restore the line to normal operations when the handset placed back on hook.
* Automatic reload capability - Required in the event of system failure. All stored program control devices must have the capability upon system recovery, from the failure to immediately initialize all system software instructions and customer specific data without outside intervention.
* Off Premise Extension (OPX) - The system provided shall accept off premise lines from distant systems and must provide OPX stations to distant locations.
* Line Lockout Feature - The system shall monitor station lines not engaged in a call for a pre-determined time and route the calling station to a receiver off-hook or intercept recording.
* Automatic Route Selection (ARS) - This feature shall provide the systems with the ability to select the most economical means to complete calls. At a minimum, ARS shall provide:
* First choice and four alternate routes
* Digit translation and routing of calls - the translated digits shall normally be an area code, city code, and an exchange code, along with the called number
* Privacy - The system shall provide a station user the capability of locking out other appearances.
* Executive Override - Except for stations protected by privacy, this feature allows a station user to break into a conversation.
* Call Detail Record (CDR) - The PBX shall provide record and store call detail information for accounting and management purposes.
* Hotline Service - The system shall provide the capability of ringing either a predetermined station or telephone/trunk outside of the system when a station equipped with hotline service goes off-hook. It shall be two-way.
* Tandem Switching Systems- Shall provide through switching for leased circuits providing off-premise service (DID to DOD) to other systems.
* Station Hunting - All telephone numbers within the system shall be capable of both station hunting and individual number selection.
* Authorization Codes - The system shall provide for an authorization code arrangement for placing long distance calls on either a voluntary/forced basis.
* Indication on Hold - The system shall be equipped to provide audible indication to all calls place on hold including camp-on calls.
* Remote Access - The user shall be able to network into an access port to access PBX features, services, or a DID trunk using a programmable access code.
* Session Initiation Protocol (SIP) Support – The system shall be able to support IP telephony signaling protocol which is used to establish, modify, and terminate VoIP telephone calls.
* Integrated Services for Digital Network (ISDN) Primary and Basic Rate Interface Access - The system shall be equipped for user-side (Primary Rate Interface (PRI) access, a T1 or E1 Primary Rate Access (PRA) facility organized into either 23 or 30 time slots of 64 kilobits per second (Kbps) each. The physical and logical interface must conform to the “I Series Blue Book” recommendations of the Consultative Committee for International Telephony and Telegraphy (CCITT). D-channel signaling through the PRI shall transmit call-handling information to the ISDN LEC central office supporting the PRA link. The switch must be able to process connections via the D-channel. The following features must be provided using D-channel signaling:
* CCITT “I and Q series” recommendations to include Recommendation No. Q.931
* 64 Kbps Clear Channel allowing the full 64 Kbps bandwidth of the time slot
* Call by call service selection (e.g., voice, data, DID, outgoing, carrier “A”, or carrier “B”)
* Station Identification Number (SID)
* Automatic Number Identification (ANI) to the Switch
* Intermodal Signaling
* The system shall support Basic Rate Interface (BRI) access and the basic rate delivery point must be provided to users at the following interface specifications:
* Terminal Equipment 1 (TE 1) at the CCITT defined S and/or T coincident reference point for user terminal equipment
* Network Termination 2 (NT 2) at the CCITT defined T reference point
* Alarm Reporting - The PBX system shall be equipped with an alarm system capable of producing visual alarms of a minimum of three notification levels, at three locations and activated by either the PBX switching hardware or the supporting power supplies. The three levels of alarm notification shall be NO ALARM, MINOR ALARM, and MAJOR or CRITICAL alarm. The three reporting locations shall be 1) in the PBX room, 2) at each console, and 3) to an internal PBX software maintenance history file record.
* Surge Suppression - All main PBX systems shall include Power Conditioner Surge Suppression and Filter for the Alternating Current (AC) power feeds for contractor-provided equipment
* CPE Categories for Consideration - Several categories of generic equipment types are commercially available. During task order performance, the contractor shall include a CPE list in each site-specific proposal. Additionally, ISDN station sets shall have flexible programmable buttons for line appearances or features and a two- line display that provides call status information and all the functionality of a key system plus the sophistication and technical advantage of ISDN capabilities.
* Station Features- At a minimum, the system shall provide the following station features:
* Automatic callback busy-lines
* Call forward, call forwarding-busy, call forwarding-no answer
* Call hold
* Call pickup
* Call transfer
* Consultation hold/three way conference
* Station speed calling
* User conference
* Call waiting
* Automatic callback busy-trunks
* Automatic ring down
* Manual line
* Message waiting
* Attendant Consoles: Each system shall be equipped with attendant console(s) designed to provide full-time and part-time operation of the overall system. Attendant console shall provide the attendant with the operation, control, and display functions and at a minimum, the features below:
  + Attendant Barge In – The attendant console shall have the capability to enter all calls, whether connected through the attendant console or dialed directly. This capability shall allow the attendant to verify the conditions of the station lines and circuit groups. The attendant console shall have the capability to establish a connection with a call-in progress. The console shall provide an identifiable tone to both parties when the attendant overrides a conversation on a busy line or trunk.
  + Busy Station Indicators –The attendant console shall be equipped with indicators capable of showing the active or inactive status of any station on the PBX.
  + Keypad – The attendant consoles shall be equipped with a keypad means of extending calls into and out of the system.
  + Dial Through – The attendant console shall be equipped to allow station users to complete the dialing of trunk calls after the attendant selects the trunk (dial-through attendant).
  + Attendant Recall – The system shall be programmable to allow unanswered calls whether on hold, camped-on, or unanswered to return to the console within a predetermined period.
  + Attendant Conference – The attendant console shall provide for, and be designed to permit, the attendant to establish up to three, independent, simultaneous conference calls, each consisting of up to five trunks and/or stations in any combination up to six parties.
  + Call Splitting – Call-splitting capability shall be provided to permit the attendant to exclude either the outside or the inside party when the attendant handles trunk calls.
  + Attendant Control of Switched Loop – Each position shall be designed so that the attendant shall have the option to extend an operator-assisted call by fixed-loop or blocked release (retains control of call until completed) or release loop (release from call once established) for all calls.
  + Console Busy Out– Each console shall have the capability of being placed in-service or taken out-of-service without affecting other consoles or system operations.
  + Display Test – Consoles shall include a visual indicator test to verify that all indicators are functional.
  + Camp-On –The attendant console shall be equipped with a camp-on feature that allows the attendant to camp-on an incoming call to a busy station. The called station shall receive a call waiting tone and, if the camped-on call is not answered within a prescribed time-period, the call shall return to the attendant for further action.
  + Busy Indication Trunks – Attendant consoles shall be equipped with visual indicators to identify an all-trunk-busy condition for each group assigned in the system.
  + Console Power – The console(s) shall include a Universal Power Supply (UPS) back-up power in the event the commercial power source fails. The contractor shall also power all features of the attendant console position(s), including all lamps and control equipment, to ensure continuous operation in the event of a commercial AC power failure for a minimum of two hours.
  + Console Display – Each attendant console shall be equipped with incoming call identification and display for discrete trunk identification, for each trunk group serving the system. Incoming calls to the attendant shall be identified by source and display information, as follows:
  + DID display trunk number
  + Other, display trunk number
  + In-house, display station number, and class of service
  + Intercept
  + Return to operator on timed recall
  + Trunk Group and Control Warning Indicators – Consoles shall provide an indication of trunk status, all trunks busy; and attendant control of the trunk group.
  + Multiple Consoles – Multiple attendant console positions shall have identical capability, and full access to all trunks and stations. In addition, consoles shall be capable of interposition transfer of calls.
  + Consolidated Consoles – Ability for a post to provide switchboard capabilities for multiple locations.
* Telephone Management System (TMS) via Virtual Private Network (VPN): Provide a management terminal and all necessary equipment and software for database changes and maintenance diagnostic checks, locally and/or remotely, that meet the following minimum functional requirements:
  + Activate/Deactivate station features
  + Activate/Deactivate trunks and stations
  + Activate/Deactivate and rearrange station lines or numbers and other actions not requiring the physical rearrangement, addition or deletion of cable, wire, or switching equipment.
  + Class of service and code restriction
  + Call pick-up and hunt groups
  + Intercom groups
  + Feature assignments
  + Maintenance/diagnostic checks
  + Trunk and trunk group availability tests
  + Provide hard copy and computer monitor display of translations and assignments
  + Remote maintenance checks and via VPN
* Provide for a voice mail system that is an integral part of the design solution.
* Provide a billing system that shall capture the call detail records of the switch and generate billing information.
* Provide a digital voice threat-recording device to each operator console, Post 1, and other designated locations.
* Mobility: Provide user mobility functionality that allows the system to simultaneously ring both the business set and an off-system telephone. The system should allow users at remote locations to call into the system, authenticate, and place calls.
  + Sites with less than 200 users – 25 users have the cell phone capability
  + Sites with 201 to 500 users – 50 users have the cell phone capability
  + Sites with 501 or more users – 100 users the cell phone capability.
* The contractor shall provide a two-level authentication for remote users to:
  + Access the system and place calls
  + Read incoming calling line ID (CLID)
  + System requests a 6-digit authorization code
* Provide analog 2-wire, 4-wire, and ethernet inter-office trunk interfaces and intra-office trunk interfaces, at the government’s direction, for integrated remotes. These trunk interfaces shall be for trunks that may connect to tie and foreign exchange lines, and the LEC for incoming and outgoing local and long-distance calls.
* The system shall support multiple signaling interface requirements including:
  + Ground Start
  + Loop Start
  + Receive and Transmit (E&M, Types I & II, Wink Start, and Immediate Start)
  + Reverse Battery Signaling
  + ISDN (Primary/Basic)
  + R2 Signaling
  + VoIP (H.323, SIP)
  + Wireless (Wi-Fi, Global System for Mobile Communications (GSM))
* Coordinate, design and interface the systems/equipment with all circuits and facilities offered by the LEC, Diplomatic Telecommunications Service/Programs Office (DTS-PO), and other communications service providers in meeting requirements of this specification.
* Engineer station, trunk, and tie line terminations associated with the equipment to conform to the requirements and standards of the LEC.
* Telephone Program Warranty, Maintenance, and License Support: All material delivered under this task order, including spares, shall have a warranty, maintenance, and license period for a minimum of three (3) years from acceptance date for replacement systems or from accreditation date for new systems.
* Repair or replacement of any item during the warranty and / or maintenance period shall be at no cost to the Government, and the contractor shall provide substitute or replacement equipment during the period of repair. These rights listed below shall be in addition to those provided by FAR 52.246-19 Warranty of Systems and Equipment.
* Telephone Program Warranty, Maintenance, and License Support: Provide a defective parts exchange process whereby:
  + Obtain a return authorization number by e-mail any weekday between 0730 hours and 1630 hours Eastern Time (ET). The plan shall include notification procedures to the Contracting Officer’s Representative (COR) of Post outages, shipping status of parts, and requests for COR assistance.
  + The contractor is liable for replacement of, and all shipping costs associated with, the replacement part to and from DOS’ Offices at SA-21 or a location within the NCR.
  + During the warranty period, the contractor shall expedite all failed components to arrive at SA-21 within the NCR within five (5) business days of receipt of failed equipment.
* Site Surveys: Provide information regarding telephone services at a specific site, where available, which may include:
  + The number of telephone systems, types of systems, location of systems installed at mission facilities.
  + The number of buildings, number of employees in each building and physical proximity of the buildings to each other.
  + Current count of extension lines, trunk lines and attendant consoles connected to each existing system.
  + The total numbers of users in the mission chancery and/or other mission facilities such as warehouse annexes and so forth.
  + The number and types (single line or multi-button) of telephone instruments currently in use in or planned for a CAA or other areas.
  + The number of direct subscriber lines in support of facsimile (FAX) machines, modems, private telephones, and other equipment that does not connect to the existing PBX or key systems.
  + Information about any additional telecommunications wire requirements beyond the one telephone and one computer wiring normally installed at each individual work area (WA) location.
  + The number of telephones, trunks, and types of systems in official residences.
  + Expected mission (Post) telecommunications requirement growth within 5 years.
  + New Embassy Compound (NEC), New Consulate Compound (NCC), New Office Annex (NOX), Lease Fit-Out (LFO) etc or other drawing packages from Overseas Buildings Operations (OBO)
* Scalability & Growth: Maintenance spares for the system shall not exceed 10% of any given electronic item, rounded up. facilitate the addition of optional equipment growth without major system/subsystem replacements, including the UPS. Provide a UPS designed for the main system to have a 2-hour run time and a 1-hour run time in the closets, when needed.
* Note: To the extent possible, parts shall be interchangeable among station equipment.
* Interoperability: Design and implement systems that interoperate fully with tie lines and with the LEC network, including International Direct Distance Dialing (IDDD), VoIP, and International Voice Gateway (IVG).
* Develop a PBX engineering configuration based on the site survey and PRS for the specific domestic or overseas site to guarantee a P-.01 grade of service (GOS) for busy hour calls between the system provided and the LEC.
* Overseas PBX: Engineer the analog or digital International Voice Gateway (IVG) to match the existing quantities of circuits plus any known increases. The systems shall typically be, but are not limited to, the following:
  + A PBX engineering configuration and installation plan based on the contractor’s recommended equipment including the following:
  + Sufficient LEC trunks to guarantee a P-.01 GOS for busy hour calls between the system provided and the LEC.
  + A trunk configuration to support a Grade P-.01 GOS for terminating calls (Tie line to station), originating calls (station to trunk or tie line), and intra-office calls (station to station).
  + IVG Circuits - The contractor shall engineer the system to match the existing quantity of analog, digital, or VOIP IVG circuits.
  + Numbering Plan - The contractor shall implement a numbering plan that:
  + Reflects the flexibility of the equipment to meet numbering plan requirements
  + Is consistent with the current IDDD, DTS-PO, as well as, LEC telephone numbering plans, as appropriate
  + Assigns extension numbers on a random basis
  + Is compatible with the numbering plan of the LEC and maintains current numbering plans, if possible. The contractor shall coordinate with the LEC regarding current and future numbering plans and shall make appropriate provisions in proposed numbering plans.
  + Includes a recommended ARS scheme based on traffic statistics and requirements, upon the lowest cost service as the first choice with the next lowest cost as the second, and so forth, and encompassing all external services and carriers
  + Includes one and/or two-digit access codes for user access to carriers and services external to the system.
  + Include direct dial access to other services (e.g., paging, radio paging, or dial dictation) implemented at the direction of the COR and included in the SSR.
  + Permit the ability to send additional digits - Once the caller obtains access to an external service the calling party shall have direct control of the circuit and shall have the ability to send additional digits.
  + A general guide for access codes (the contractor may recommend different codes for some locations and shall not exceed three digits).

Table

Description automatically generated

* Familiarization Session(s): Provide a familiarization session plan as part of the SSR describing procedures (including number of familiarization sessions, number of instructors, number of personnel at each session, and length of sessions) to adequately accomplish technical overview and familiarization sessions as mutually agreed upon. Familiarization sessions shall be provided to the following groups of personnel:
  + Attendant Console Operators - familiarize the Attendant Console Operators as part of the attendant Console installation process prior to system cutover.
  + System Management Staff - provide a systems overview for the local management staff with a system overview after the contractor advises that the system is installed and ready for use, and prior to cutover. The overview shall cover system orientation for the telephone manager and assistants, the principles, theory, and structure of the system, as well as demonstrations of equipment operations. In addition, this orientation shall cover operation of the TMS and management terminals, including data base entry and the most commonly implemented system software changes.
  + Executive Level Managers – provide system orientation for executive level managers as indicated in the site survey report and directed by the Post POC.
  + General Users Familiarization - provide familiarization to general users in all features of the new system operation, both system and station features as indicated in the site survey report. Provide the attendance records of the familiarization sessions as specified.
  + RIMC and Other Staff - provide a systems overview for the RIMC Field Technicians and other identified staff. Conduct the basic system overview, which cover system orientation for the telephone manager and assistants, the principles, theory, and structure of the system, demonstrations of equipment operations. In addition, this orientation shall cover operation of the TMS and management terminals, including data base entry and the most commonly implemented system software changes.
* Familiarization Session(s): Submit all changes to the approved familiarization session outlines, procedures, and documentation to the COR for approval at least thirty days prior to conducting the sessions.
* Familiarization Session(s): Provide Familiarization Session(s) on how to use equipment delivered, including but not limited to:
  + Voicemail
  + Auto Attendant
  + UPS
  + Station Equipment
  + Apparatus
* Familiarization Session(s): Provide appropriate user flyers or manuals in a quantity of one per telephone plus 10 percent.
* Familiarization Session(s): Provide station instrument push button faceplates indicating access codes for telephone system station features for each station instrument.
* Inspection and Acceptance Criteria: Perform a traffic analysis for five business days on all new main systems to determine adequacy of trunking and inter and intra office calling to finalize the trunking configuration.
* Inspection and Acceptance Criteria: Provide a trunks usage report indicating no maximum or peak usage of more than 90 percent of the wired and installed trunk ports to identify all provided excess circuits.
* Inspection and Acceptance Criteria: The acceptance period for exiting Posts shall be a continuous 7-day period of no system hardware generated major alarms or loss of call processing for the PBX.
* The acceptance period shall conclude a minimum of two business days after installation of the final key system, if the Post has any off-compound system installed
* Provide an industry-standard and compliant, high-performance structured telecommunication infrastructure equipment, design, and solution that meets or exceeds all current DOS and industry standards and accommodates DOS mission requirements and applications. Equipment shall meet at minimum the following:
  + All cable to the desktop must be CAT-6 or better
  + All backbone cable must be OM-3 or better
  + All outside plant (OSP) cable must be either OM-3 or OSP-1 or better
* Deliverables include but are not limited to:
  + Site Survey Report (Includes the PRS, Draft Site Survey Report (DSSR) and the Final Site Survey Report (FSSR)
  + Communications (e.g., Briefings, Deep Dives, Cables, Incident Reporting)
  + Post Installation Report (PIR)

## Regional Relay Facility (RRF) Support

Regional Relay Facility (RRF) Support responsibilities ensure that the IT systems and substructure within the Region Relay Facility (RRF) Telecommunications Center Facility (TCF) hosting vital networking and Telecommunications assets for Department of State (DOS) and its other government agency (OGA) partners remain sufficiently secure, robust, scalable, and efficient to deliver integrated services throughout the underlying physical environment.

### General RRF Support Requirements

* Manage and support the RRF, keeping the services stable, high performing, and secure.
* Operate, maintain, and monitor all components of the services and interfaces with other services and systems.
* Fulfill service requests, respond to incidents, and resolve problems related to these services.
* Provide Infrastructure Engineering support to optimize capacity, availability, performance, stability, security, and usability of the services and underlying systems to meet evolving Department requirements.
* Maintain service and system documentation and knowledge base materials.
* Provide expedited response to automated DCIM alerts (ex. Power, cooling, etc.) related to issues and/or failures reported by intelligent power and environmental monitoring devices.
* Identify and protect system boundaries (i.e., Space, Power, cabling, physical access) established by system owners having equipment located within the Telecommunications Center.
* Maintain system owner and ISSO responsibilities for the Authorization and Assessment (A&A) process Follow and participate in standard ITIL best practices and ISO 20K standards to maintain the services.
* Perform all tier 2 and 3 support in accordance with the DOS ITSM processes and using DOS ITSM tools, including the use of the enterprise ticket system and internal change processes for incident tracking and change approval.
* Organize and conduct quarterly Internal Process Audits (IPAs) and participating in External Independent Process Audits conducted by Independent Third Parties.

### Relay Infrastructure Management Support

* Conduct analysis, processing, tracking, and coordination of various customer requests (i.e. change/incident/service) and maintenance/testing activities
* Provide response to and/or assistance with fulfilling requests; Tracking and reporting responses to incidents that result in change and service requests.
* Perform coordination of routine activities such as site visits for technical surveys, system installations, and scheduled maintenance/repairs of equipment/infrastructure with applicable internal/external stakeholders (ex. Requesters, support staff, management, etc.).
* Execute preparation of documentation associated with planned changes (i.e., Change Requests, Drawings/Schematics, status reports, etc.).
* Support tracking of change related activities, communication/collaboration with customers and stakeholders
* Conduct verification of delivery and quality checks of operational work products based on customer change and service requests; Provides outcome verification reporting on if changes were completed as planned and within schedules or resulted issues.
* Participate in the acquisitions process as required by evaluating/testing products/services of potential vendors during market research, interfacing with potential and existing vendors, and providing feedback on benefits and shortcomings of acquisition targets.
* Participate in the acquisitions process as required including construction of procurement requests (PR), input for acquisition justifications, conducting market research, and interfacing with potential and existing vendors.

### Regional Relay Facility Change Management and Data Center Management

* Sustain maintenance of Configuration Management (CM) databases containing data on Configuration Item (CI) records that includes CM info for internal/external agency assets located within the Telecommunications Center and their associated network connections.
* Manage access to network shares/drives containing folders/files for organization sensitive information that includes CM related data.
* Execute Infrastructure database verification, CI database entry, and other CM tasks associated with the execution of change requests.
* Perform quarterly CM audits of CI records and correcting discrepancies.
* Support activities within the RRF’s Local Change Control Board (LCCB) in regard to hardware/firmware/software baseline changes originating from Change Requests; Ensures that proposed changes to documentation are properly reviewed and processed through the LCCB.
* Maintain all processes and procedures relating to best industry practices of CM to include support for external audits.
* Conduct technical reviews of change requests for adding, modifying, or removing supported IT devices (ex. networking, security appliances) and related infrastructure.
* Create infrastructure design documents and recommendations for cost effective improvements to supporting infrastructure that maintain efficiency, security, and enforcement of applicable compliances (i.e., DOS, federal, and industry).
* Provide support to Data Center Infrastructure Management (DCIM) Technician and systems/tools Administration activities used to manage, maintain, and track rack, connectivity, power, and environmental substructure necessary for the proper operation of core systems/services housed within the RRF’s TCF.

### Network Services Center - Network Encryption Services

* Provide onsite and remote management Tier II and Tier III engineering/technical support for Inline Network Encryption (INE) services, including firmware upgrades, baseline security configuration changes, loading and updating of keying material and device audit services.
* Provide Tier II and Tier III engineering/ technical support and remote management/ monitoring of all Classified networks and INE devices (Foreign and Domestic) along with providing Operations and Maintenance (O&M) support.
* Provide encryption domain monitoring, hardware and network fault isolation, and service restoration of Type I Inline Network Encryption (INE) devices, which often requires Tier II and Tier III engineering technical support.
* Provide Tier II and Tier III Engineering management, technical assistance, O&M support/ services, and on-site dispatch to various local (MD/DC/VA) supported annexes and customers to repair and resolve Classified Network INE issues. Also provide custodial and O&M services for select dedicated core customers.
* Conduct site visits to current and future annexes/customers for INE welfare checks, site surveys, emergency customer assistance, user familiarization training, and verification of INE installations/modifications.
* Analyze the surveys of Domestic Classified sites the NSC is responsible for, to continue towards establishing a high-level strategy for the classified integration to allow for the Domestic and Foreign Classified Core to remain integrated into one network and allow the network to continue under configuration Control.

### COMSEC Office of Record services/COMSEC child account manager services

* Provide account oversight, policy, and administration audit services to include site visits for the purpose of COMSEC custodian inspections, point of contact confirmations, and delivery of equipment/materials.
* Provide receiving/tracking of COMSEC inventory (i.e., equipment and keying materials), processing COMSEC equipment transfers, and destruction of sensitive materials under inventory.
* Provide execution of Unit Security Officer (USO) responsibilities under physical access management to include combination changes (i.e., Container and room access), processing visitor access requests.
* Provide Security Requirement Reviews, Briefings, Training, Risk Management/Reporting, and planning related to Disaster Recovery (DR) and Continuity of Operations (COOP).
* Provide additional COMSEC management support for 20 external Annexes.

### COMSEC Inline Network Encryption (INE) Support

* Provide technical support, on site and/or remote INE management.
* Provide technical support for INE maintenance, firmware upgrades, baseline security configuration changes, loading and updating of keying material and device audit services.
* Provide device/encryption domain monitoring, hardware and network fault isolation, and service restoration of Type I Inline Network Encryption (INE) devices.
* Complete site visits of all for the purpose of INE welfare checks, site surveys, emergency customer assistance, user familiarization training, and verification of INE installation/modification of current and future annexes/customers, for which the COMSEC office is responsible.
* Provide continued monitoring and technical helpdesk Inline Network Encryptor (INE) support.

### COMSEC Secure Voice Terminal equipment Support

* Provide technical support for Secure Voice Terminal equipment maintenance, firmware upgrades, baseline security configuration changes, loading and updating of keying material and device audit services.
* Provide hardware fault isolation and service restoration of Type I Secure Voice Terminal equipment Onsite Secure Voice Terminal equipment management.
* Complete site visits for the purpose of Secure Voice Terminal equipment welfare checks, site surveys, emergency customer assistance, user familiarization training, and verification of installation/modification of current and future annexes/customers, for which the COMSEC office is responsible.

## Cybersecurity Management

Cybersecurity management services shall include, but are not limited to, compliance and reporting, risk management, and access management for network services.  Compliance and reporting encompass the guidance and standards developed by the National Institute of Standards and Technology (NIST) in compliance with the Federal Information Security Modernization Act (FISMA).  Risk management identifies and prioritizes risks to minimize the impact of vulnerabilities and to ensure the proper configuration of information systems.  Finally, access management is the selective restriction of permissions to a network or local resource via policies and controls.

### Cybersecurity Management Support

* Define cloud Cybersecurity and Information Assurance requirements and policies.
* Provide Cybersecurity governance and administration.
* Support Cybersecurity governance and administration by executing on best practices in accordance with guidance from DOS.
* Prepare and update System Security and Contingency Plans for OpenNet and ClassNet that conform to the NIST-800 standards and are stored in Xacta or similar GRC tool.
* Prepare and update the Self-Assessment for DOS networks that conforms to the NIST-800 standards.
* Perform technical vulnerability assessments involving sophisticated tools and procedures to identify specific configuration and implementation weaknesses within the network infrastructure.
* Ensure that system designs address solutions that are securable. Provide support for Security Architects and Engineers.
* Proactively assist DOS with identifying security products, services, and requirements that meet DOS’ business needs and address emerging risks.
* Provide input for updating the Plan of Action and Milestones (POA&Ms) for security weaknesses identified into Xacta or similar GRC tool. This plan shall conform to IA and OMB standards.
* Work closely with the DOS to ensure network systems maintain Security Assessment and Authorization (A&A).
* Develop security enhancements and provide security engineering to minimize network vulnerability to unauthorized intrusions and denial-of-service attacks and implementing intrusion testing to identify vulnerabilities.
* Contribute to the development and execution of test strategies, test plans, test cases/scripts, and test reports for effective security testing of IT Management systems.
* Work with other DOS entities to resolve any security vulnerability issues and support DOS Continuous Diagnostics and Mitigation (CDM).
* Recommend best practice threat intelligence policies, maintenance, and optimization.
* Support analysis and develop cybersecurity recommendations to address ongoing and emerging issues, innovation, and automation.
* Respond to data calls and other reporting requirements using prescribed DOS tools and proposing new and innovative tools and solutions where appropriate.
* Provide cybersecurity SME support to respond to Binding Operational Directives (BOD), updates to NIST standards, updates to OMB requirements, and other requirements in the federal regulatory environment.

### Compliance and Reporting

* Provide Cybersecurity Policy Subject Matter Leadership in Cybersecurity Governance policy and enterprise standards including the review and comment on Governance related issues.
* Support efforts for innovation and automation of federal-mandated compliance and reporting activities.
* Manage the Assessment and Authorization (A&A) process for information systems.
* Support DOS GRC planning, reporting and audit activities from integrated security and risk management perspective.
* Provide thought leadership to identify opportunities to strengthen DOS integrated risk management capabilities.
* Obtain and actively maintain A&A across network solutions to ensure compliance and support efforts to move towards Ongoing Authorization.
* Prepare and update self-assessments for information systems. These assessments shall conform to the NIST-800 standards.
* Create, track, and close Plan of Action and Milestones (POA&M) for information systems in coordination with Subject Matter Experts (SME).
* Work with SMEs on system documentation such as System Security Plan (SSP) and Information System Contingency Plan (ISCP) along with other A&A security artifacts.
* Prepare and facilitate ad hoc vulnerability scans as needed based on emerging threats and provide results to DOS.
* Present cybersecurity metrics, inspection metrics, and enterprise risk management measures via dashboards for situational awareness.
* Review Security Impact Assessment (SIA) requests for information systems in coordination with SMEs.
* Advise SMEs on best practices to resolve security control findings for information systems.
* Document additional security needs and requirements as they are discovered, or gaps are identified.
* Maintain a Cybersecurity Improvement Plan which consists of approved mitigations, and participate in self-assessments and surveys, implement, and track corrective action plans for all reportable findings.
* Manage FISMA quarterly reports based on the Chief Information Officer (CIO) metrics and Cybersecurity Framework (CSF).
* Enter and verify information into the Xacta or similar GRC workflow tool to describe information systems. Promotes the Risk Management Framework.
* Proactively recommend and implement continuous improvements to the services provided to DOS during the term based on achievement of the agreed upon KPIs.

### Cybersecurity Risk Management

* Oversee periodic reviews of information system risk level.
* Gather reports of targeted areas with high-risk scores from stakeholders.
* Coordinate systematic reviews of audit logs per DOS and federal regulations.
* Reports on vulnerabilities and anomalies discovered to the Information System Security Officer.
* Coordinate response to cybersecurity incident.
* Monitor, track, and communicate Security Event and Security Incident summary and reports back to DOS (e.g., immediate report, root cause analysis report, monthly summary reports).
* Investigate and report on cybersecurity events and incidents to DOS senior management, Cyber Incident Response Team (CIRT), and Cybersecurity Operations (IRM/CO) as necessary.
* Establish supporting tools and processes to enable secure retention of evidence to support forensic investigations.
* Coordinate with other government agencies as a part of incident response teams or sharing of information received from intelligence sources.
* Interface with incident response teams in the Federal and State Governments, and international incident organizations.
* Develop dashboards for monitoring the cybersecurity health of information systems.
* Ensure dashboards abide by the NIST-800 standards and are coordinated with the CDM program and support efforts for innovation and automation.
* Oversee the periodic execution of Contingency Plan exercises to ensure stakeholders have awareness of their roles and responsibilities.

### Access Management

* Coordinate access for personnel including activation, changes, and terminations.
* Manage access control matrix to document rights and permissions.
* Conduct monthly or quarterly reviews to validate that personnel access to DOS security infrastructure, programs and libraries is appropriate for named systems.
* Promote separation of duties through technical (i.e., Role Based Access Control [RBAC]) or manual means (i.e., authorized approving official).
* Clear on elevated rights (includes enterprise and system tool administrator) accounts for staff after approval by an authorized approving official.
* Utilize proper tools to set the correct privileged access rights to elevated rights and service accounts used by the information systems.
* Administer the network device access process for tokens and accounts used after clearance by an authorized approving official.
* Supervise the stale (i.e., unused, or inactive) accounts process for elevated rights and service accounts used.
* Support efforts for the Department to transition to:
  + Zero Trust based on OMB and DHS principles and playbooks
  + Innovations, emerging technologies, and automation
  + Multi-factor Authentication
  + Identity Governance and Administration, may include support for machine identities
* Provide for Access Management analytics to provide historical information about all administration and runtime access events; Can include user and entity behavior analytics (UEBA).
* Provide timely notification of separation of all personnel with access to DOS data or security infrastructure. Access to data and/or security infrastructure should be terminated in accordance with DOS’ policies and procedures.

## Data Warehouse, Business Intelligence and Asset Discovery

Data warehouse, business intelligence and asset discovery responsibilities shall include, but are not limited to, facilitating the storage and processing of structured and unstructured data for query, analysis, inventory, and reporting purposes. Data warehouses and the data they contain are carefully planned and assembled to deliver specific business analysis and decision-making results. Data warehousing and Asset Discovery will focus on centralized data storage of while business intelligence is concerned with data analysis and presentation. Accommodations must be made for the various types of structured and unstructured data, the technologies supporting the data and where the data is stored, whether state-hosted (on-premises, device, and applications), mobile, endpoints or outsourced (cloud containers). The following table identifies the roles and responsibilities.

### Data Warehouse

* Provide Data Warehousing, Business Intelligence and Asset Discovery to facilitate the storage and processing of data for query, analysis, inventory, and reporting purposes for use by the Cyber Integrity Center, Cyber Operations, Diplomatic Security, and other organizations. (Includes both structured and unstructured data).
* Make accommodations for the various types of structured and unstructured data, the technologies supporting the data and where the data is stored, whether state-hosted (on-premises, device, and applications), mobile, endpoints or outsourced (cloud containers).
* Define data quality requirements, prioritizing mission critical systems and their data. Note: Data quality may vary depending on business needs of application.
* Establish robust data quality standards and procedures for the data input process.
* Perform continuous data quality monitoring and assessments of poor data and the expense of future remediation. Utilize data quality tools appropriate for the system and data being monitored.
* Perform data corrections as defects are discovered. When possible, utilize automated processes to implement corrections.
* Assess and understand data security requirements. This assessment must consider business needs, data classifications, potential threats, compliance, and the availability of data security technologies.
* Plan, install, configure, and maintain environments for structured and unstructured data.
* Acquire and ingest data into data storage environments.
* Develop, enhance, and maintain data backup and recovery plans. Plans must address data loss, data corruption, and data hardware failures scenarios.
* Ensure the data warehouse system obtains Security Authorization and Accreditation (A&A) and once obtained to ensure that the status remains up to date.
* Identify and document DOS requirements for business data analysis and reporting. Include sources for business analysis data.
* Develop, enhance, and maintain the data warehouse and business intelligence infrastructure. Solutions must be architected to include the technologies (servers, storage, and software), standards, and procedures necessary to sustain successful implementation, including tools for data extraction and loading, data quality, metadata management, and data analysis and reporting.
* Prepare data (e.g., discover, gather, cleanse, transform) for business analysis and reporting.
* Extract, cleanse, transform, and load data into the data warehouse.
* Monitor and tune data warehouse and business intelligence process for performance.
* Develop and manage discovery dashboard for self-service reporting. Dashboard Management includes but is not limited:
  + Governance and control of access and privileges based on DOS guidance/policy
  + Validating data and addressing integrity concerns

### Business Intelligence

* Configure business intelligence analysis and reporting capabilities.
* Design, develop, document process and procedures for system users and administrators.

### Asset Discovery

* Use asset discovery tools to identify and document all IT assets on all DOS networks and cloud environments
* Design, setup, engineer, manage, deploy, improve, document, and implement changes to discovery infrastructure.
* Upgrade and patch hardware and software and recover and monitor the Discovery infrastructure.
* Provide ad hoc reporting upon request if data is available or not readily available in discovery dashboard.
* Resolve customer (e.g., systems owners, system administrators for all Post and Bureaus) issues related directly or within the scope of being a discovery issue.
* Control access and privileges of users to discovery dashboard.
* Validate integrity of all data output of discovery infrastructure.

## Transition Services

Transition services responsibilities shall include, but are not limited to, activities such as transition planning, knowledge transfer, etc. required to successfully transfer ownership from the outgoing vendor to the incoming vendor and/or to DOS.

### Transition-in Services

* Understand and comply with DOS policies and procedures throughout Transition.
* Recommend an overall Transition methodology and Project Plan to accelerate and expedite service transition.
* Provide a communications plan for all Government stakeholders (Office/Division/Branch) with resources under this task order.
* Provide input to the Project Plan and coordinate input of DOS Vendor Partners.
* Perform all knowledge transfer activities necessary to assume the Services under this Task Order.
* Work with DOS and DOS’s current vendors to transfer, innovate, and/or assign rights under any existing equipment or software or other contractual agreements necessary to assume the Services under this Task Order, as applicable.
* Assume responsibility for the performance of all services in accordance with the Statements of Work and SLRs under this Task Order.
* Put in place all operational systems and supporting tools necessary to perform the Services under this Task Order.
* Mitigate any and all risk or possibility of outage of any service or system that could be caused by transition activities.

### Transition Out Services

* Review and provide input to the Transition methodology and Project Plan developed by the subsequent vendor at the end of the Task Order.
* Provide a communications plan for all Government stakeholders (Office/Division/Branch) with resources under this task order.
* Perform all Knowledge Transfer activities necessary to transition the Services under this Task Order to the subsequent vendor.
* Work with DOS and the subsequent vendor to transfer, innovate, and/or assign rights under any existing equipment or software or other contractual agreements necessary to transition Services under this Task Order, as applicable.
* Assist the subsequent vendor to mitigate any and all risk or possibility of outage of any service or system that could be caused by transition activities.

## Cross-Functional Requirements

The following table summarizes the Cross-Functional categories that all contractors are required to support across each task order.

Table 2.1 – Cross Functional Requirements

| **Requirements Category** | **Description** |
| --- | --- |
| IT Compliance | IT Compliance resources setting policy, establishing controls and measuring compliance to relevant legal and compliance requirements. Includes but is not limited to: Governance, Risk & Compliance, Business Continuity & Disaster Recovery. |
| Security | IT Security resources setting policy, establishing process and means, measuring compliance and responding to security breaches. Includes Identity & Access Management, Security Awareness, Cybersecurity & Incident Response, Threat & Vulnerability Management, and Data Privacy & Security |
| Disaster Recovery | IT Disaster Recovery resources setting DR Policy, establishing process and means, dedicated failover facilities, performing DR testing: NOTE: DR designated equipment is included directly in its own sub-tower (e.g., extra servers for DR are included in Compute tower, etc.). |
| Client Management | Resources or “account managers” aligned with the lines of business to understand business needs, communicate IT products, services and status of IT projects. |
| IT Service Management | Resources involved with the incident, problem and change management activities as part of the IT Service management process (excludes the Tier 1 help desk). |
| Product and Project Management | Resources involved with managing and supporting IT related projects and/or continuous product development (e.g., Agile) across business and IT-driven initiatives. |
| Innovation, Ideation, and Modernization | The investment, development, and incubation of new technologies to create new or better solutions which meet unarticulated or existing market needs. Includes new technology solutions and new product incubation services.  Includes enterprise architecture solutions that enhance and modernize DOS services. |

### IT Compliance

IT Compliance resources include setting policy, establishing controls and measuring compliance to relevant legal and compliance requirements. This includes but is not limited to: Governance, Risk & Compliance, Business Continuity & Disaster Recovery.

The Contractor shall:

1. Comply with all relevant certification and accreditation requirements and documentation specified by DOS and the U.S. Government.
2. Adhere to policies and procedures defined in the Foreign Affairs Manual (FAM) and associated Foreign Affairs Handbooks (FAHs) to include, but not limited to proactively reporting non-compliance issues and risks.
3. Participate in compliance, risk and regulatory governing bodies, processes and activities as required.
4. Measure (or provide inputs needed to support measurement of) compliance to relevant legal and compliance requirements.
5. Monitor all work performed by assigned Contractor personnel to ensure the ongoing and continuous incorporation of and adherence to all appropriate Compliance requirements.
6. Report on compliance in coordination with other DOS stakeholders and/or Contractors.
7. Support remediation of compliance discrepancies as directed.
8. Support the definition and establishment of controls to monitor compliance.

### 508 Compliance

The Contractor shall ensure the system is compliant with Section 508 throughout the implementation and integration of the work to be performed. The Contractor shall ensure the system is compliant with all appropriate 508 requirements and lead the testing and validation for every major and minor release. In the event that a user with disabilities identifies a defect with 508 compliance the Contractor must accommodate appropriately. Section 508 of the Rehabilitation Act of 1973, as amended (29 U.S.C.794d) requires that when Federal agencies develop, procure, maintain, or use electronic information technology, Federal employees with disabilities have access to and use of information and data that is comparable to the access and use by Federal employees who do not have disabilities, unless an undue burden would be imposed on the agency.

Section 508 also requires that individuals with disabilities, who are members of the public seeking information or services from a Federal agency, have access to and use of information and data that is comparable to that provided to the public who are not individuals with disabilities, unless an undue burden would be imposed on the agency.

Applicable standards are 1194.211194-26.

Implementation Instructions

* <http://www.section508.gov/content/learn/laws-and-policies>
* <http://www.access-board.gov/508.htm>
* <http://www.w3.org/WAI/Resources>

### Security

IT Security resources setting policy, establishing process and means, measuring compliance and responding to security breaches. Includes Identity & Access Management, Security Awareness, Cybersecurity & Incident Response, Threat & Vulnerability Management, and Data Privacy & Security.

### Information Technology Security Plan

In accordance with Dept of State Acquisition Regulation (DOSAR) clause 652.239-71(b), the contractor shall develop, provide, implement, and maintain an IT Security Plan.

### Cybersecurity

Cybersecurity is mandatory for all task orders placed under the Evolve contract. The objective of the cybersecurity requirement is to ensure that all task orders placed under the Evolve IDIQ not only comply with DOS standards but go above and beyond those requirements to consider how to make DOS systems more resilient and secure in the face of continuously changing threats. The following are the current cybersecurity standards, frameworks and policies that will apply at the task order level as applicable. These lists are not all inclusive and are subject to change:

1. Federal Information Processing Standards Publications

| Federal Information Processing Standards Publications (FIPS Pub) | Reference |
| --- | --- |
| Security Requirements for Cryptographic Modules | FIPS Pub 140-3 |
| Standards for Security Categorization of Federal Information and Information Systems, February 2004 | FIPS Pub 199 |
| Minimum Security Requirements for Federal Information and Information Systems, March 2016 | FIPS Pub 200 |
| Personal Identity Verification of Federal Employees and Contractors,” January 24, 2022 | FIPS Pub 201-3 |

1. National Institute of Standards and Technology Publications

| National Institute of Standards and Technology (NIST) | Reference |
| --- | --- |
| Guide for Applying the Risk Management Framework to Federal Information Systems:  A Security Life Cycle Approach, June 10, 2014 | NIST SP 800-37 |
| Security and Privacy Controls for Federal Information Systems and Organizations, January 22, 2015 | NIST SP 800-53 Rev. 4 |
| A Recommendation for the Use of Personal Identity Verification (PIV) Credentials in Physical Access Control Systems, November 20, 2008 | NIST SP 800-116 |
| Digital Identity Guidelines, June 2017 | NIST SP 800-63-3, 800-63A, 800-63B, 800-63C |
| Guidelines for Derived PIV Credentials, December 2014 | NIST SP 800-157 |
| Guidelines on Hardware-Rooted Security in Mobile Devices (Draft), October 2012 | NIST SP 800-164 |
| Draft National Institute of Standards and Technology Interagency Report - Mobile, PIV, and Authentication, March 2014 | NISTIR 7981 |

1. Office of Management and Budget Publications

| Office of Management and Budget (OMB) | Reference |
| --- | --- |
| Managing Federal Information as a Strategic Resource,” July 28, 2016 | OMB Circular A-130 |
| Continued Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors, February 3, 2011 | OMB Memorandum M-11-11 |
| Transition to IPv6, September 28, 2010 | OMB Memorandum |
| Acquisition of Products and Services for Implementation of HSPD-12, June 30, 2006 | OMB Memorandum M-06-18 |
| Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors, August 5, 2005 | OMB Memorandum 05-24 |
| Safeguarding Against and Responding to the Breach of Personally Identifiable Information, May 22, 2007 | OMB Memorandum M-07-16 |
| Implementation of Trusted Internet Connections (TIC), November 20, 2007 | OMB Memorandum M-08-05 |
| Securing the Federal Government’s Domain Name System Infrastructure, August 22, 2008 | OMB Memorandum M-08-23 |
| Improving the Federal Government’s Investigative and Remediation Capabilities Related to Cybersecurity Incidents August 27, 2021 | OMB Memorandum M-21-31 |
| [Identity, Credentialing, and Access Management (ICAM)](https://www.whitehouse.gov/wp-content/uploads/2019/05/M-19-17.pdf), May 2019 | OMB Memorandum M-19-17 |

1. Security Policies

| Security Policies | Reference |
| --- | --- |
| "Trusted Internet Connections (TIC) Reference Architecture Document, Federal Interagency Technical Reference Architectures, Department of Homeland Security, ([https://www.doi.gov/sites/doi.gov/files/uploads/tic\_ref\_arch\_v2-0\_2013.pdf](https://gcc02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.doi.gov%2Fsites%2Fdoi.gov%2Ffiles%2Fuploads%2Ftic_ref_arch_v2-0_2013.pdf&data=04%7C01%7CWeakley-LugoKF%40state.gov%7C14aea13923b646e405db08d96bae63f1%7C66cf50745afe48d1a691a12b2121f44b%7C0%7C0%7C637659219012429211%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C1000&sdata=YbP5%2FAfsntmTWA2EUBBBFCR5F8gVqSLDiifPXpmWiWs%3D&reserved=0)) " | Version 2.0, October 1, 2013\*Version 3 in draft |
| "Trusted Internet Connections (TIC) https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/omb/memoranda/fy2008/m08-05.pdf" | OMB M-08-05 |
| "Domain Name System Security (NSSEC) https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/omb/memoranda/fy2008/m08-23.pdf" | OMB M-08-23 |
| Federal Information Security Modernization Act (FISMA) of 2014 | 44 U.S.C. § ch.35 |
| Clinger-Cohen Act of 1996 also known as the Information Technology Management Reform Act of 1996 | 40 U.S.C |
| Privacy Act of 1974 | 5 U.S.C. § 552a |
| Homeland Security Presidential Directive, “Policy for a Common Identification | HSPD-12 |
| Standard for Federal Employees and Contractors, August 27, 2004 |  |
| Management of Federal Information Resources, and Appendix III, | (OMB) Circular A-130 |
| Security of Federal Automated Information Systems”, as amended | OMB Circular A-130 | |
| E-Authentication Guidance for Federal Agencies | OMB Memo M-04-04 | |
| Standards for Security Categorization of Federal Information and Information Systems | FIPS PUB 199 | |
| Minimum Security Requirements for Federal Information and Information Systems | FIPS PUB 200 | |
| Security Requirements for Cryptographic Modules | FIPS PUB 140-3 | |
| Guide for Developing Security Plans for Federal Information Systems | NIST Special Publication 800-18 Rev 1 | |
| Risk Management Guide for Information Technology Security Risk Assessment Procedures for Information Technology Systems | NIST Special Publication 800-30 | |
| Contingency Planning Guide for Information Technology Systems | NIST Special Publication 800-34 | |
| Guide for the Security Certification and Accreditation of Federal Information Systems | NIST Special Publication 800-37 | |
| Security Guide for Interconnecting Information Technology Systems | NIST Special Publication 800-47 | |
| Recommended Security Controls for Federal Information Systems | NIST Special Publication 800-53 | |
| Guide for Assessing the Security Controls in Federal Information Systems | NIST Special Publication 800-53A | |
| Voice Over Internet Protocol (VoIP) Telephony | CNSSI 5000 | |
| Voice over Secure Internet Protocol (VoSIP) | CNSSI 5000 ANNEX I | |
| Softphone Security Requirements | CNSSI 5000 ANNEX J | |
| Type-Acceptance Program for Voice Over Internet Protocol (VoIP) Telephones | CNSSI 5001 | |
| Telephony Isolation Used for Unified Communications Implementations Within Physically Protected Spaces | CNSSI 5002 | |
| National Instruction for Approved Telephone Equipment | CNSSI 5006 | |
| Telephone and Security Equipment Submission and Evaluation Procedures | CNSSI 5007 | |
| Safeguarding Communications Security (COMSEC) Facilities and Materials | CNSSI 4005 | |
| Enabling Mission Delivery through Improved Identity, Credential, and Access Management | OMB Memo M19-17 | |
| Cybersecurity Strategy and implementation Plan (CSIP) | OMB Memo M16-04 | |
| Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure | E.O 13800 | |
| Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information | E.O. 13587 | |
| Instruction for National Security Systems (NSS) Public Key Infrastructure (PKI) X.509 Certificate Policy, Under CNSS Policy No. 25 | CNSSI 1300 | |

The contractor is responsible for remaining abreast of all new mandatory cybersecurity requirements at both the federal and DOS level and complying with the requirements relevant to this task order.

In addition to being able to perform in accordance to the referenced publications as required at the Task level for sensitive data and information technology (IT) resources, a contractor shall ensure that the contractor's information security policies, procedures, and practices applicable to all information systems it owns or operates which contain, transmit, or process information provided by or generated for the Government to support the operations and assets of a Federal agency (“Federal Information”), and which may be reasonably contemplated to be used during the performance of this contract, meet, at a minimum, the requirements of the security control baseline for Low-Impact information systems (in the most current version of NIST Special Publication 800-53), or conform to commercial standards requirements that provide a substantially equivalent or greater level of security.

### Disaster Recovery

Disaster Recovery services are the services and activities required to prevent and/or respond to a disaster event through the restoration of key computing functions as swiftly and smoothly as possible. A “disaster event” in this context is any event that prevents a mission-critical system from maintaining an operational state at the client production data center.

The Contractor shall:

1. Design, maintain, update, and enhance IRM’s business continuity for all IT Services detailed in Continuity of Operations Plan (COOP) and demonstrated Disaster Recovery (DR) capability to maintain the same level of operational support and ensure that the alternative capability meets SLAs and COOP guidelines.
2. Coordinate the involvement of all Vendor and third-party resources managed by the Vendor in the development, maintenance, testing, and execution of the disaster recovery and COOP plan.
3. Develop, evaluate, and maintain a Disaster Recovery Plan IAW IRM COOP and NIST SP 800-34 and review and update annually.
4. Ensure changes are accurately reflected in Continuity of Operations Plan (COOP) and Disaster Recovery (DR) as necessary.
5. Develop, maintain, test, and support disaster preparedness, high availability, and recovery procedures in accordance with the IRM hosted server environment.
6. Provide a single point-of-contact upon the declaration of a Disaster to coordinate with DOS or their designee and all appropriate third parties

### Client Management

Client Management includes resources or “account managers” that are aligned with the lines of business to understand business needs, communicate IT products, services, and status of IT projects.

The Contractor shall:

1. Designate a single point of contact to liaise directly with the Program Offices utilizing services delivered via this Task Order.

### IT Service Management

The Portfolio Management task order provides overarching ITSM activities for the task orders executed under the other Evolve functional categories. See PWS Section 2.1.1 for ITSM requirements for the subject task order.

### Program and Project Management

The Portfolio Management task order provides overarching Program, Product, and Project Management activities for the task orders executed under the Evolve IDIQ contract vehicle across functional categories. See PWS Section 2.1 for Program and Project Management requirements for the subject task order.

### Innovation, Ideation, and Modernization

The investment, development, and incubation of new technologies to create new or better solutions which meet unarticulated or existing department needs. Includes new technology solutions and new product incubation services.  Includes enterprise solutions that enhance and modernize DOS services.

The Contractor shall:

1. Supply value engineering reports as needed.
2. Provide the most cost effective, efficient, state-of-the-art, integrated turnkey solutions while incorporating practical innovations and technologies.
3. Determine and develop best practice processes by building upon ones already in place at IRM to improve operational efficiency.
4. Identify, develop, and advance the IRM vision and strategic plan to reform IT acquisitions by bringing industry standard best practices and driving innovations.
5. Ensure IRM remains current with evolving requirements and technology advances

# Special Requirements / Instructions

## Standards (e.g., 5 FAM 600)

The Contractor shall ensure that all work is completed in accordance with U.S. government and Department of State standards, policies, procedures and guidelines as provided.

## Government-Furnished Equipment / Information

The Government may furnish workspace and other appropriate furnishings, computer hardware and software, telephones and other material appropriate to the performance of tasks. Any Government furnished materials, data, or property shall remain the property of the Government and will be returned upon completion of the support services. Government furnished equipment shall be tracked through applicable procedures that will be provided by the Contracting Officer in accordance with the Federal Acquisition Regulation (FAR).

## Place of Performance

Work under this task order shall be performed primarily at DoS facilities in the Washington, DC metropolitan area, including primarily State Annex (SA-34) at 7374 Boston Blvd., Springfield, VA 22153, the Harry S. Truman Building and other State Annexes in the Washington, DC area. Additional support may be required at the State Annex 26 in Beltsville, MD and/or the ESOC West Data Center in Denver, Colorado and SA-20 – Rosslyn.

The Government authorizes offeror personnel to telework for the performance of their work functions. If telework or remote work is contemplated for the performance of tasks in this PWS, it shall be conducted per Government telework policies and be authorized by the COR or the CO.

## Period of Performance

This task order comprises a one-year base performance period, with up to four, one-year option periods.

Base Year:

Option Year 1:

Option Year 2

Option Year 3:

Option Year 4

## Standard Work Hours

The Department normal work hours are 8:15 a.m. to 5:00 p.m., Monday through Friday. Contractor personnel are to be available both during normal working hours and as required for after-hours on-call support, when approved in advance by the GTM.

Unless other hours are specified in the task order, hours of performance on the contract will be an 8-hour workday, excluding lunch, but start times may vary depending on the task assignment. The Contractor will be required to cover the core hours from 0900 to 1500, Monday through Friday. During times of emergency and under unusual conditions, i.e. declared emergencies, civil unrest etc., the Contractor shall be prepared for 24-hour performance.

## Security Clearance Requirements

Contractor personnel assigned to this contract shall possess up to a **TOP SECRET** with Special Compartmented Information **(SCI)** personnel security clearance issued by the Defense Counterintelligence and Security Agency (DCSA) commensurate with the level of access required, prior to contract performance. All Contractor personnel supporting this contract will possess at least the minimum-personnel security clearance issued by the Defense Security Service commensurate with the level of access required and as specified in the DD Form 254, prior to contract performance, unless otherwise notified.

Security clearance requirements for contractors accessing DoS information systems shall be in accordance with Volume 12, Foreign Affairs Manual, Section 600. Furthermore, while at DoS locations, the Contractor shall comply with applicable DoS regulations relative to the protection of classified and/or sensitive information. The Office of Information Security (DS/IS/ISP/INB) is responsible for inspecting the Contractor’s activities with at Department locations.

Contractor personnel shall meet the personnel security clearance requirements identified in the DD-254 and task order/s. Most contractor personnel supporting the contract are expected to have a SECRET level security clearance, at a minimum. Additional security clearance requirements may be stipulated by the GTM. The prime or, in the case of a joint venture (JV), the owners of the JV (all primes) must have a TOP SECRET facility clearance by the date of the proposal submission, or it will be considered non-compliant. Subcontractors do need a cleared facility based on the highest-level clearance of their employees.

Visit requests are to be sent to DS/IS/ISP/INB, SA-20, 13th floor, Rosslyn, Virginia 22209. Letters of Consent issued by the Defense Security Service must be attached to all Visit Authorization Requests (VARs). All DD Form 254 for subcontracts shall be forwarded to DS/IS/ISP/INB for certification prior to issuance to the subcontractor.

See the contract clauses and DD 254 for the complete security requirements.

### Personnel

Vendor shall provide and maintain appropriately skilled staffing to meet the Networking Services Roles and Responsibilities and Service Level Requirements set forth in this PWS.

* Most personnel require a Top-Secret security clearance. For some specific projects, a Top-Secret clearance with SCI is required. Depending on the assignment or effort, a minimum of Public Trust is required. Clearances should be planned at the minimum required level of the position.
* All personnel must be familiar with and follow all physical security requirements and guidance and comply with directions issued by the Unit Security Officer (USO).
* All personnel visiting a foreign country under this task order shall abide by existing practices of obtaining official “Country Clearance.”
* All personnel shall provide for the protection of Classified and Sensitive But Unclassified (SBU) communications commensurate with federal and Department of State (DOS) policies, regulations, and standards.

The vendor shall maintain and provide regular notifications on all clearances and additional pre-requisites for personnel which can include: Top-Secret Cryptographic Access, NATO security clearances, Visit Authorization Request (VAR), and Authorization Request (AR) and any other applicable documentation prior to providing support.

To support excellence in delivery of service to the enterprise, the Vendor will proactively manage talent by ensuring a comprehensive set of capabilities, certifications, clearances, and expertise as defined by DOS. Workforce planning should include but is not limited to talent acquisition and onboarding, talent development and performance management, as well as succession planning.

## Non-Disclosure Agreement

The Contractor shall sign a non-disclosure agreement with the Department of State when working with sensitive and/or proprietary information (forms to be executed and maintained by the Contracting Officer Representative (COR)). The Contractor and its employees shall exercise the utmost discretion in regard to all matters relating to their duties and functions. The Contractor shall not communicate to any person any information known to them by reason of their performance of services under this task order which has not been made public, except in the necessary performance of their duties or upon written authorization of the contractor officer.

All documents and records (including photographs) generated during the performance of work under this task order shall be for the sole use of and become the exclusive property of the U.S. Government. Furthermore, no article, book, pamphlet, recording, broadcast, speech, television appearance, film or photograph concerning any aspect of work performed under this task order shall be published or disseminated through any media without prior written authorization of the contracting officer. The contractor shall include the substance of this provision in all contracts of employment and in all subcontracts.

## Organizational Conflict of Interest (OCI)

**Determination:** The Government has determined that this effort may result in an actual or potential conflict of interest or may provide one or more Offerors with the potential to attain an unfair competitive advantage. The nature of the conflict of interest and the limitation on future contracting (description to be included in task order request).

If any such conflict of interest is found to exist, the TO Contracting Officer may (1) disqualify the Offeror, or (2) determine that it is otherwise in the best interest of the United States to contract with the Offeror and include the appropriate provisions to mitigate or avoid such conflict in the task order awarded. After discussion with the Offeror, the TO Contracting Officer may determine that the actual conflict cannot be avoided, neutralized, mitigated or otherwise resolved to the satisfaction of the Government, and the Offeror may be found ineligible for award and if the task order has already been awarded and new information comes to light such as a Corporate Change as described in section f, the government may terminate the contract for connivence.

**Disclosure:** The Offeror hereby represents to the best of its knowledge that:

* + 1. \_\_\_\_It is not aware of any facts which create any actual or potential organizational conflicts of interest relating to the award of this task order, or
    2. \_\_\_\_It has included information in its proposal, providing all current information bearing on the existence of any actual or potential organizational conflicts of interest, and has included the mitigation plan in accordance with paragraph (d) of this provision.

**Mitigation/Waiver:** If an Offeror with a potential or actual conflict of interest or unfair competitive advantage believes it can be mitigated, neutralized, or avoided, the Offeror shall submit a mitigation plan to the Government, IRM/BMP/ITA/CM, for review. Award of a contract where an actual or potential conflict of interest exists shall not occur before Government approval of the mitigation plan. If a mitigation plan is approved, the restrictions of this provision do not apply to the extent defined in the mitigation plan. If not defined, then this provision applies fully.

**Other Relevant Information:** In addition to the mitigation plan, the TO Contracting Officer may require further relevant information from the Offeror. The TO Contracting Officer will use all information submitted by the Offeror, and any other relevant information know to DOS, to determine whether an award to the Offeror may take place, and whether the mitigation plan adequately neutralizes or mitigates the conflict.

**Corporation Change:** The successful Offeror shall inform the TO Contracting Officer and Evolve Program Manager within thirty (30) calendar days of the effective date of any corporate mergers, acquisitions, and/or divestures that may affect this provision.

**Flow-down:** The contractor shall insert the substance of this clause in each first-tier subcontract that exceeds the simplified acquisition threshold.

## Associate Contractor Agreements

Within the first 30 days of task order award the contractor shall provide a draft ACA to the Evolve Program Manager for review and approval. An example is provided in Attachment J-7, Associate Contractor Agreement Sample.

Table in paragraph (g) below will be populated once prime task order contract awardees are known.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(a) The Contractor shall enter into Associate Contractor Agreements (ACA) for any portion of the contract requiring joint participation in the accomplishment of the Government’s requirement. The agreements shall include the basis for sharing information, collected mission requirements, code, data, technical knowledge, expertise, and/or resources essential to the integration of the Evolve

Program and individual task order objectives, software baselines, and components, which shall ensure the greatest degree of cooperation for the development of the program to meet the terms of the contract. Associate contractors are listed in paragraph (g) below.

(b) ACAs shall include the following general information (See template to utilize):

(1) Identify the associate contractors and their relationships.

(2) Identify the program involved and the relevant Government contracts of the associate

contractors.

(3) Describe the associate contractor interfaces by general subject matter.

(4) Specify the categories of information to be exchanged or support to be provided.

(5) Include the expiration date (or event) of the ACA.

(6) Identify potential conflicts between relevant Government contracts and the ACA; include

agreements on protection of proprietary data and restrictions on employees.

(7) Identify the process through which contractors will ensure interoperability of processes and technology used under each task order. For example, ensuring that no tool can only be operated by one contractor

(c) A copy of such agreement shall be provided to the awardees by the Government for review

before execution of the document by the cooperating contractors. All awardees need to collaborate on finalized ACA.

(d) The Contractor is not relieved of any contract requirements or entitled to any adjustments to

the contract terms because of a failure to resolve a disagreement with an associate contractor.

(e) Liability for the improper disclosure of any proprietary data contained in or referenced by any agreement shall rest with the parties to the agreement, and not the Government.

(f) All costs associated with the agreements are included in the negotiated cost of this contract.

Agreements may be amended as required by the Government during the performance of this

contract.

(g) The following contractors are associate contractors with whom agreements are required:

1. Associate Contractors

|  |  |  |
| --- | --- | --- |
| Contractor | Address | Program/Contract |
|  |  |  |
|  |  |  |

## Travel

Personnel assigned to this contract may be required to travel. All officially directed travel, per diem and associated miscellaneous expenses required as a result of work performed under this task order shall strictly adhere to all Government travel regulations. Travel is receipt reimbursable. Unless otherwise specified in the task order, travel to work locations within 50 miles of the National Capital Beltway (495) is considered local travel and will not be reimbursable.

## Other Direct Costs

Other direct costs may be required to deliver the services in this PWS.

## Funding

This task order will be incrementally funded.

## Invoice Approval

The Government Task Manager (GTM) must approve all invoices before submission for payment.

## Technical Direction

Guidance and specific direction in carrying out the stated requirements will be provided by the COR on an ongoing basis. Contractor personnel will be expected to carry out instructions received from the COR in a professional and timely manner. The Government will not provide counseling to contractors on their conduct; it is assumed that once the Contractor receives technical direction about how to perform duties that the Contractor will implement the instructions.

## Required Languages

English is the current required language.

# Task Order Management

## Key Personnel

The Contractor shall identify key personnel and provide resumes for the positions identified as key personnel for this task order. If the proposed key personnel are not current employees, then the resume must be accompanied with a signed letter of intent that states the prospective employee has authorized their resume to be submitted, intends to accept employment if the Offeror is selected for award, and that the parties have agreed to salary parameters. If any of the key personnel candidates become unavailable at any point during the evaluation process, the Offeror shall immediately notify the Contracting Officer. The contractor shall be able to replace key personnel within 15 business days. Replacement requires government approval and personnel must meet same criteria as the original employee.

Listed below are minimum key personnel considered essential to the performance of work for this Task Order.

1. Task Order Key Personnel

| Labor Category | Description |
| --- | --- |
| Task Order Program Manager | Acts as a single technical point of contact (POC) who shall work closely with the Government Program Manager (PM), Contracting Officer Representative (COR), and Government Technical Monitor (GTM).  **The Task Order PM shall:**   * Be ultimately responsible for ensuring the Contractor’s performance meets all task order requirements. * Have the requisite authority for full control over all company resources necessary for task order performance. * Have the authority to approve task order modifications in emergent situations. * Be ultimately responsible for personnel management, management of Government material and assets, and personnel and facility security. * Demonstrate progressive IT experience in the functional area of the task order. At least one project shall have occurred within the past three (3) years of similar scope with a total contract value greater than $10M and global delivery in a highly complex environment. Oversight or management of at least one project shall have been conducted in accordance with a CMMI certified, Agile, and ITIL approach. * Demonstrate proven experience and documented success supervising large IT services contracts, including people of various job categories and skills. * Demonstrate expertise in the management and control of costs and resources and demonstrated capability in managing projects of this type and complexity. * Demonstrated experience providing system modernization and innovation that resulted in increased operational efficiency or cost savings. * Manage and maintain contractor interface with the senior levels of the customer’s organization. * Consult with customer and contractor personnel to formulate and review task plans and deliverables, ensuring conformance with program and project task schedules and costs and contractual obligations. * Establish and maintain technical and financial reports to show progress of projects to management and customers, organize and assign responsibilities to subordinates, oversee the successful completion of all assigned tasks, and assume the initiative and provide support to marketing personnel in identifying and acquiring potential business.   **Minimum qualifications:**   * Demonstrated proven experience and documented success supervising large IT services contracts, including people of various job categories and skills. * Demonstrated expertise in the management and control of costs and resources and demonstrated capability in managing projects of this type and complexity. * Demonstrated experience providing system modernization and innovation that resulted in increased operational efficiency or cost savings. * 10 years of relevant experience * Bachelor’s degree in a related field, with a preference for a Master’s degree in Business Administration (MBA) or Information Technology * ITIL Certified * PMP Certified (current) * Agile certification highly desired |

## Substitution of Key Personnel

The Contractor shall notify the TO CO and the TO COR prior to making any changes in Task Order Key Personnel. No changes in TO Key Personnel will be made unless the Contractor can demonstrate that the qualifications of prospective replacement personnel are equal to or better than the qualifications of the TO Key Personnel being replaced. All proposed substitutes shall have qualifications equal to or higher than the qualifications of the person to be replaced. The TO CO shall be notified in writing of any proposed substitution at least forty-five (45) days, or sixty (60) days if a security clearance is to be obtained, in advance of the proposed substitution. Such notification shall include:

1. an explanation of the circumstances necessitating the substitution;
2. a complete resume of the proposed substitute; and
3. any other information requested by the TO CO to enable him/her to make a key personnel replacement determination

The Evolve Program Manager and the contract level CO will evaluate substitutions at the contract level and the TO CO and TO COR will evaluate TO level substitutions. Requests will be reviewed promptly the Contractor will receive timely written notification of his/her approval or disapproval in writing. All disapprovals will require resubmission of another substitution within 15 calendar days of receipt of the written denial by the Contractor. The Contractor shall allow a minimum of a two-week transition of key personnel.H.11 Insurance

Insurance of the following kinds and minimum amounts shall be furnished at any time at the request of the CO and maintained during the period of performance of this contract:

1. Worker's compensation and employer's liability. The Contractor shall, as a minimum, meet the requirements specified at (FAR) 48 CFR 28.307-2(a).
2. General liability. The Contractor shall, as a minimum, meet the requirements specified at (FAR) 48 CFR 28.307-2(b).
3. Automobile liability. The Contractor shall, as a minimum, meet the requirements specified at (FAR) 48 CFR 28.307-2(c).

## Meetings/Conferences

### Task Order Kick-Off Meeting

The purpose of the Kick-Off Meeting is to achieve a clear and mutual understanding of all task order requirements and to identify and resolve potential problems.

The Contractor shall:

* Attend a task order kick off meeting convened by the Government, onsite or virtual, within 30 days after task order award
* Introduce key personnel during the meeting and present management and risk management processes to be used under the task order, addressing key risks to include dependencies and mitigation for each identified risk
* Update and present the following:
  + - Updated Transition-In Plan
    - Updated Project Management Plan
    - Master Milestone Schedule
    - Associate Contractor Agreement(s)
    - Updated Earned Value Management Plan (if applicable)
    - Agile Reporting Tool (if applicable)

The CO is responsible for establishing the time and place of the conference and will notify the appropriate Government representatives and the Contractors. The Evolve Program Manager will designate or act as the chairperson at the conference. The chairperson of the conference shall conduct the meeting.

The conference may be conducted at a location within the Washington, DC commuting area or completely online at the Government’s discretion.

## Task Order Deliverables

1. Unless the Government identifies otherwise, all deliverables must be submitted in English and in electronic, Microsoft Office compatible, format via email.
2. The Government will review each deliverable product and may provide oral and written comments. The Contractor shall review and incorporate comments or implement directed changes no later than five (5) business days thereafter. This time period may be extended, at the sole discretion of the Government, by written approval of the Contracting Officer or COR (if responsibility has been delegated by the CO).
3. All documentation and reports developed or provided by the Contractor shall become the property of the U.S. Government. Reports shall not contain any markings or legends which will restrict the Department’s use of such reports in any way. All deliverables, including attachments, shall comply with the data right clauses incorporated in the contract. The Government will reject all deliverables containing markings contradicting said clauses.
4. Deliverables longer than 5 pages shall include a table of contents. Attachments, if any, shall include the attachment number, deliverable name and number, and contract number and task order number.
5. For purposes of delivery, all deliverables shall be made by close of business (COB) 4:30 P.M. local time (Washington, DC) at destination, Monday through Friday, unless stated otherwise.
6. All deliverables submitted in electronic format shall be free of any known computer virus or defects. If a virus or defect is found, the deliverable will not be accepted. The replacement file shall be provided within two (2) business days after notification of the presence of a virus.
7. Each deliverable shall be accompanied by a cover letter from the Contractor. Multiple deliverables may be delivered with a single cover letter describing the contents of the complete package.
8. In the event the Contractor anticipates difficulty in complying with any task order-level deliverable, the Contractor shall provide written notification immediately to the task order-level Contracting Officer and TO COR. Each notification shall give pertinent details, including the date by which the Contractor expects to make delivery; PROVIDED, that this data shall be informational only in character and that receipt thereof shall not be construed as a waiver by the Government of any contract delivery schedule, or any rights or remedies provided by law or under this contract.
9. Schedule of Deliverables

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Deliverable | Section Reference | Due Date | Update Frequency | Distribution |
| Associated Contractor Agreement | 3.9 | 30 days after every new task order award and updated as applicable | As needed | Evolve Program Manager |
| Labor Allocation Report | 4.5 | As requested | Monthly |  |
| Meetings/Conferences (Meeting notes/action items) | 4.3, 4.7 | 3 working days after meeting / conference | As required | CO, TO COR, Evolve Program Manager |
| Project Management Plan, to include Quality Control Plan | 4.9 | Within 30 calendar days after TO award (Draft) | Annually, or upon request |  |
| Service and Incident Reports | 4.7 | As required | As required |  |
| Task Order Kick Off Meeting (Draft Schedule) | 4.4 | Prior to task order start date | N/A |  |
| Task Order Monthly Status Reports | 4.10 | 1 month after award of first task order | Monthly | CO, COR, Evolve Program Manager |
| Transition-in Plan | 4.8.1 | 30 calendar days from award of first task order | One-time | TO CO, TO COR, TO CPM |
| Transition-out Plan | 4.8.2 | NLT 120 calendar days prior to the end of contract or 60 calendar days following the Government’s request | One-time | TO CO, TO COR, TO CPM |
| Quality Assurance Surveillance Plan | 5.3.2 |  |  |  |

## Labor Allocation Report

Personnel assigned to this TO will track the time worked aligned to projects or programs assigned by the Government. This allocation, done at the hourly level, shall consist of the following information:

* Employee name
* Employee CLIN
* CLIN bill rate
* Number of hours worked in support of each project code

Project codes are Government-assigned codes that are aligned to projects, programs, and efforts for labor to be recorded against, and the contractor should be able to bill against new project codes within 2 business days. Administrative time that is not billed against the Government should be noted appropriately. In the absence of a Government-assigned code, the CO or COR shall provide direction for billing that time period until project codes can be assigned.

Reporting period will be monthly. The report will be provided in an Excel or comparable format with the data unlocked and ready to be ingested into Government reports.

The Contractor shall provide individual timesheet as requested by the Government CO or COR.

The Contractor is accountable to established performance metrics and the quality-of-service criteria for deliverables within respective service areas. This could be a general statement that addresses the holistic needs of all sections under ENM or a breakout of Key Result Areas (KRAs) with their Key Performance Indicators (KPIs) and Critical Success Factors (CSFs).

These reports may be used for evaluating if contract staff are meeting organizational requirements for project support. Contract staff whose organizations measure performance based on how time is spent on projects aligned to organizational goals and fail to meet project milestones may be removed for failure to perform, in coordination with the CO or COR.

## Service and Incident Reports

The contractor shall provide monthly reports from the IT Service Management System for any staff whose work involves responding to ITSM requests. Reports shall be provided to the Branch and/or Division Chief of the work unit and be customized as needed for that organizational unit. Roll up reports of the same data provided to Divisions and Branches will be provided for the Office-level (or higher) Government staff.

These reports may be used for evaluating if contract staff are meeting organizational requirements for service, support, and development. Contract staff whose organizations measure performance based on ticket metrics and fail to meet organizational goals may be removed for failure to perform, in coordination with the CO or COR.

## Meeting Minutes

Sharing meeting minutes as a record of information shared at the meeting is a guiding principle for the task order.

All formal meetings’ minutes for staff in an organizational unit shall be shared with Office Directors of the organizational unit at a minimum, either via email or, with the Office Director’s concurrence, a shared online repository. If meetings are informal or non-recurring, then requirements for meeting minutes will be determined by the Government staff in the meeting. Meeting minutes may be shared with additional Government personnel as requested by team leads, Government leadership, GTMs, and COR/COs. Meeting minutes will only be used for evaluating contract staff if that requirement is coordinated with the GTM prior to the start of the meeting and should not be used as a primary performance source.

## Task Order Transition

### Transition-In Plan

The contractor shall develop a Transition-in Plan that details activities that shall be completed no later than 30 calendar days from the effective date of performance.

The Transition-In Plan shall include the following:

* Planned transition activities
* Transition activity timelines and milestones
* Transition resource requirements (includes the retention of current staff, as applicable and appropriate)
* Transition security implications
* Transition risks and mitigation or avoidance strategies; and
* Transition notifications and training of users

### Transition-Out Plan

The contractor shall develop a Transition-out Plan that facilitates the accomplishment of a seamless transition from the incumbent to an incoming contractor/Government personnel at the expiration of the contractor.

The contractor shall provide a final Transition-Out Plan NLT 120 calendar days prior to the end of the contract, or 60 calendar days after the Government requests the deliverable.

The Transition-Out Plan shall include the following:

* Project management processes
* Points of contacts
* Location of technical and project management documentation, data, and methods of providing these to these to the incoming service provider
* Status of ongoing technical initiatives
* Appropriate contractor-to-contractor coordination to ensure a seamless transition
* Transition of Key Personnel
* Schedules and milestones
* Actions required of the Government
* Methods of measuring transition risks that includes a complete inventory of the transition risks, with assigned severity and probability, and response plans to address the risks either through avoidance, mitigation, or other means
* Method of permitting the successor service provider to observe and become familiar with any and all operation specified in this PWS for a minimum of 120 calendar days prior to the expiration or termination of the contract
* Method of establishing and maintaining effective communication with the incoming service provider for the period of the transition via weekly status meetings; and
* Method for ensuring that all information assets and related configuration information is up-to-date and available for the Government’s review at least 120 calendar days prior to the end of the contract

## Project Management Plan

The Project Management Plan (PMP) shall define policies and procedures for managing and directing the effort for productivity, quality, cost control, and early identification and resolution of problems. The PMP shall include schedules, milestones, tasks, and subtasks required in the PWS.

* The PMP shall provide a Work Breakdown Structure (WBS) or epics with user stories, and associated roles and responsibilities of the Contractor.
* The PMP shall include the Contractor’s Quality Control Plan (QCP), Transition Plan Overview, and the stakeholder management and communication plan. The Contractor shall provide the Government with an initial PMP draft.
* The Contractor will be prepared to review and discuss the initial PMP outline at the Project Kick-Off Meeting. The PMP is a “living document” and shall be updated as necessary to reflect current tasks, objectives, and deliverables. The Contractor shall work from the latest Government approved version of the PMP

## Task Order Monthly Status Reports (MSR)

The Contractor’s PM shall develop and provide an MSR via electronic mail to the CO, COR and GTM by the 10th of the following month. The Contractor shall consult with the COR on the format of the report. The MSR shall include, at minimum, the following:

* Activities during reporting period, by task (include: on-going activities; new activities; activities completed; progress to date on all above-mentioned activities). Start each section with a brief description of the task
* Problems and corrective actions taken. Also include all new and pending issues or concerns and proposed resolutions to address them
* Personnel gains, losses, and status
* Government actions required
* Project schedule (major tasks, milestones, deliverables, planned and actual start and completion dates, etc.)
* List of all documents submitted during reporting period to include version number and last revision date.
* If applicable, submit a summary of trips taken, conferences attended, etc.

At the CO’s, COR’s, or GTM’s request, a monthly status meeting may be held. In addition, the contractor shall meet as necessary with the government to discuss progress and problems. These meetings shall enable problems to be identified and resolved quickly. The contractor shall document the problems and the solutions.

# Performance Requirements

## Quality of Reports and Deliverables

General quality measures, as set forth below, will be applied to each work product received from the Contractor under this contract.

1. Accuracy: work products shall be accurate in presentation, technical content, and adherence to accepted elements of style.
2. Clarity: work products shall be clear and concise. Any/all diagrams shall be easy to understand and be relevant to the supporting narrative.
3. Consistency to Requirements: All work products must satisfy the requirements of this contract and specific task orders.
4. Timeliness: work products shall be submitted on or before the due date specified herein or submitted in accordance with a later scheduled date determined by the Government.

## Acceptance Criteria and Inspection

Acceptance of all written documents and other deliverables will be contingent upon Government Task Manager (GTM) review and approval. The GTM will discuss each specific task with the Contractor to ensure that the goals and objectives are clearly defined. Required graphs, charts, columns, and rows of data shall be legible and properly formatted. Unless valid justification is cited to the contrary, the GTM comments will be incorporated into the respective final documents and reports. If GTM comments given, do not conform to safe business practices or are deemed technically unsound; it is the responsibility of the Contractor to advise the GTM. Consensus is required between the GTM and the Contractor; however, if consensus is not achieved, actions will be as directed by the GTM.

Upon approval of the final draft, deliverables will be submitted in final form to the GTM. All deliverables shall be delivered to the GTM in both hard copy and electronic format, which will be determined upon contract award.

## Quality Control and Quality Assurance

### Quality Control

The contractor shall develop and maintain an effective quality control program to ensure services are performed in accordance with this PWS. The contractor shall develop and implement procedures to identify, prevent, and ensure non-recurrence of defective services. The contractor’s quality control program is the means by which it assures that the work complies with the requirement of the contract.

After acceptance of the quality control plan the contractor shall receive the contracting officer’s acceptance in writing of any proposed change to his QC system.

### Quality Assurance

The Government will utilize several quality assurance procedures to ensure contractor compliance with this task order, as detailed in attachment J-X: QASP. The QASP sets forth the procedures and guidelines that the Department of State, Bureau of Information Resources Management will use in ensuring the required performance standards or services levels are achieved by the contractor

Examples include inspection of deliverables, review of reports, and onsite progress meetings, performance evaluations, etc. to ensure that, at a minimum, the PWS requirements have been met; sufficient consideration has been given to alternative approaches for implementing the components of the project; and defensible explanations have been provided to justify recommendations, etc.

The contractor shall maintain the highest degree of quality for all activities performed throughout the period of performance of the task order. The Government shall regularly evaluate the Contractor’s performance including, but not limited to:

* Inspections of deliverables identified within this PWS for completeness, accuracy and timeliness; note that it is the Contractor’s responsibility to ensure adherence to the submitted QCP to ensure acceptable performance under the award.
* Assurances that validated and correct implementation strategies have been selected for the program.
* The contractors’ ability to retain quality individuals to perform the contact requirements.

# Appendix A: Basic Performance Standards

# Overview

The contractor shall meet all the requirements listed in this PWS. Specific minimum performance requirements are listed for some tasks. Where specific minimum requirements are not listed, the basic standard is assumed to be an accurate, timely, high-quality product that effectively performs its intended function. The Government may review performance on any and all requirements contained in this PWS. Failure to meet the basic performance standards could result in administrative actions

# Employee Technical Performance

**Source**: Each individual staffed on the contract effectively meets the requirements of their position as it is detailed in this Performance Work Statement

**Measurement**: The GTM/COR will direct routine meetings with Office/Division/Branch staff to discuss business at which time staff will report on their duties. The GTM/COR will also interact with staff on a daily basis and observe their performance and conduct as well as consider input from other Government staff to ensure that contractor staff are meeting contractual obligations with effective performance and sound conduct and will act accordingly and document as necessary. Evaluation of this quality consideration will be subject to the COR’s best informed judgement.

# Employee Customer Service

**Source**: Each individual staffed on the contract provide effective customer service to the clients of IRM- domestic, overseas, and external - per their duties in the Performance Work Statement

**Measurement**: This contract will be evaluated on the overall customer service skills of its staff. Multiple measurements will be used for this evaluation including survey feedback pertaining to both general use of network services and specific offerings staffed by this contract, oral or written input provided to by customers to Government management, and the best judgment of the COR observing performance. ServiceNow (or other ticketing system) metrics will be used when available.

# Project Management

**Source**: Any pertinent projects assigned by the COR to staff on the contract pertaining to network services should be thoroughly documented in technical specifications, using Agile project plans, and completed by assigned deadlines, barring sufficient justification to do otherwise.

**Measurement**: Projects requiring deadlines will be assigned in writing by the GTM/COR for which contract staff will provide technical specifications, project plans, and timely status updates in writing as necessary and written notification upon approval. Any proposed justifications for extending the deadline will be requested in writing to the GTM/COR who will then approve or disapprove the extension in writing. GTM/COR will make note of any projects not meeting deadlines without approval.

# Staffing Management

**Source**: When replacements to currently budgeted staff are needed or the Government requests additional staff provided for in the contract, contract management act with reasonable promptness and effectiveness to consider and then hire quality personnel. The Government reserves the right to view the resumes of prospects that the contractor considers to be best qualified, request to meet selections of those candidates, and to provide feedback to the contractor regarding those candidates.

**Measurement**: The GTM/COR will document his/her best judgment on the timeliness of the contractor’s response to filling a vacancy need and as pertinent, document opinions on the quality of proffered candidates. Generally, the Government would prefer to see 3-5 resumes per vacancy. Generally, the Government would prefer to minimize disruptions caused by vacancies, which should be filled in a timely manner.

# Performance Measurement

Program office performance will utilize a combination of operational metrics and customer-facing metrics. The operational metrics are Government-defined metrics, subject to change, that measure day-to-day technical and business value. The customer-facing metrics are the SLAs that IRM has with their customers. The DOS may, for its internal purposes, manage, provide oversight, and assess overall performance of the task order. The Contractor shall recommend and adhere to DOS-approved policies, procedures, measurement and evaluation practices, and monitoring and reporting requirements for managing IT infrastructure components and applications to obtain optimal performance.

# Operational Metrics

The following operational metrics are a set of measurements used to aid in the day-to-day monitoring and management of IT services. These metrics are a living, internal Government framework that is provided by the Government to the Contractor to facilitate clear communication about the Government’s plans with regard to routine oversight and assessment.

| **IRM Metrics** | | | | |
| --- | --- | --- | --- | --- |
| **Performance Evaluation Category** |  |  |  | |
| **Performance Based Metrics** | **Detailed Description** | **Program Office Quality Level** | |
| **Target Met** | **Target Exceeded** |
| **Task Order Performance** | Business protected against violations/ infractions | This measurement is designed to count the number of violations or infractions committed by the vendor and reported to the service desk, ISSO, or other legitimate authority. “Violations or Infractions” consist of security breaches, as defined in 12 FAM 590 and 12 FAM 550, as well as lack of compliance with the rules of behavior outlined in the annual Security Awareness Training (PS800) provided by the Foreign Service Institute.   Frequency: Monthly   This measurement will be applied throughout the life of the project. | 0 Violations and Infractions | N/A |
| **Task Order Performance** | Timely Hiring of Staff | The contractor replaces departing personnel within 14 days of the employee’s departure. | 8-14 days | 0-7 days |
| **Task Order Performance** | Turnover Ratio | Contractor shall strive to minimize overall staff attrition and maintain organizational knowledge to the maximum extent possible | 5% monthly staff attrition over last twelve months or life or contract – whichever is less | 2% monthly staff attrition over last twelve months |
| **Program Management** | Project Management Variance (CV & SV) | Percent Cost Variance (CV) and Schedule Variance (SV) at each phase of development   CAPA Control: 14.99% | Control: +/- 5.0% | Exceed: < 4.99% |
| **Program Management** | Requirements Artifacts | Planned vs. Actual Delivery of Requirements Artifacts. Excludes Artifacts with valid change record(s).   CAPA Control: > 3 days from planned | Control: +1-3 days from Planned | Exceed: < 1 days from Planned |
| **Program Management** | Testing Artifacts | Planned vs. Actual Delivery of Testing Artifacts. Excludes Artifacts with valid change record(s).   CAPA Control: > 3 days from planned | Control: +1-3 days from Planned | Exceed: < 1 days from Planned |
| **Systems Development** | Design and Development | Average Code Review Checklist form results. The Code Review Checklist will be completed for each promotion of code/solution from Development to Test and Test to Production. The items on the form will be based on Design and Development standards TBD by the Design and Development team.   CAPA Control: > 20% out of compliance | Control: 5-20% out of compliance | Exceed: < 5 % out of compliance |
| **Systems Development** | Customer Satisfaction | CAPA Control: 1.9 | Control: 2.0-4.6 | > 4.7 |
| **Systems Development** | Defects introduced to Production | # of Defects introduced to Production per Release   CAPA Control: 5+ | Control: 0  Major or Critical, 1-5 all other Severity | Exceed: 0 |
| **Enterprise Service Operations** | Assessment and Authorization (A&A) | All A&A activities delivered according to IA quarterly deliverables. This metric will be measured and reported quarterly but applies throughout the life of the project. | No more than 1 missed deliverable per quarter | Zero missed deliverables per quarter |
| **Enterprise Service Operations** | Mean Time Between Failure | Mean Time between Failures (in hours) [unplanned] Defined by an outage caused at the application layer. Time between 2 outages. | >360 hours | >504 hours |
| **Enterprise Service Operations** | Mean Time to Recover | Mean Time to Recovery (in minutes) [unplanned]. The average of all recovery times/number of outages. | <65 minutes | <40 minutes |
| **Enterprise Service Operations** | Hours over Planned Outage | Aggregated hours over quarter exceeding planned scheduled maintenance. Actual amount of hours for maintenance vs. scheduled hours of maintenance. This metric will be measured and reported quarterly. | <4 hrs. | <2.25hrs |
| **Enterprise Service Support** | Incident Resolution – High Priority | Percentage of tickets completed within 12 hours for High Priority tickets | >/= 90% (or one with less than 10 tickets) | >93% |
| **Enterprise Service Support** | Incident Resolution – Routine | Percentage of tickets completed within 24 hours for all ticket categories | >90% | >93% |
| **Enterprise Service Support** | Incidents Reopened | Percentage of tickets reopened within 24 hours | <5% | <3% |
| **Enterprise Service Support** | Initial Incident Response | Initial response time from ticket assignment to customer service response | <120 min/ticket average (2 hours) | <60 min/ticket average (1 hour) |
| **Enterprise Service Operations** | iPost Score (OpenNet) | iPost score captured every Tuesday at the CCB and then take the average for the Month.   (35 = A) | <22 | <19 |
| **Enterprise Service Operations** | iPost Score (ClassNet) | iPost score captured every Tuesday at the CCB and then take the average for the Month.  (1750 = A+) | <1750 | <875 |