**SAMPLE – For Reference Only** – This sample is a redacted copy of a work statement accomplished under a NITAAC GWAC. A Statement of Work (SOW) is typically used when the task is well-known and can be described in specific terms. Statement of Objective (SOO) and Performance Work Statement (PWS) emphasize performance-based concepts such as desired service outcomes and performance standards. Whereas PWS/SOO's establish high-level outcomes and objectives for performance and PWS's emphasize outcomes, desired results and objectives at a more detailed and measurable level, SOW's provide explicit statements of work direction for the contractor to follow. However, SOW's can also be found to contain references to desired performance outcomes, performance standards, and metrics, which is a preferred approach. **This sample is not all inclusive, therefore the reader is cautioned to use professional judgment and include agency specific references and regulations to their own PWS/SOO/SOW.**

Information Technology Support

Performance Work Statement (PWS)

# Introduction

## Background

Enter background information here.

## Purpose

The tasks areas covered by the PWS are:

* Task Order Management Services
* Program Management Office (PMO) Services
* IT Policy, Administration and Regulatory (ITP) Services
* IT Operations and Maintenance Support Services
* Information Security and Systems Assurance (ISSA) Services
* Systems Engineering (SE) Support Services

## Contract Type

Enter type of contract here.

## Period of Performance

Enter type of contract here.

## Government Furnished Equipment (GFE)/ Government Furnished Information (GFI)

The Government intends to provide the contractor several operational hardware and software systems, network management tools, and databases. These are GFE.

The Contractor’s management staff shall be responsible for keeping track of Government Furnished Equipment (GFE) assigned to its staff in accordance with <AGENCY> property management. <AGENCY> will use financial and legal penalties for missing GFE regardless of the circumstance (e.g., theft, fire, and flood) in accordance with FAR 52.245-1.

## Scope of Work

CIO-SP3 Task Areas:

Task Area 1: IT Services for Biomedical Research, Health Sciences, and Healthcare

Task Area 2: Chief Information Officer (CIO) Support

Task Area 3: Imaging Task Area 4: Outsourcing

Task Area 4. Outsourcing

Task Area 5: IT Operations and Maintenance Task Area 6: Integration Services

Task Area 7: Critical Infrastructure Protection and Information Assurance

Task Area 8: Digital Government

Task Area 9: Enterprise Resource Planning

Task Area 10: Software Development

# Program Goals

## CIO Organization

Describe the program goals for the CIO Organization here.

## Guiding Principles

<AGENCY> has identified several key guiding principles for the ITS contract, including:

* **Quality Execution:** The Contractor shall deliver and maintain reliable information technology services for <AGENCY> stakeholders.
* **Customer Service:** The Contractor shall be dedicated to customer service and adept at meeting schedules in a dynamic and changing marketplace.
* **Cost Control:** The Contractor shall maintain mechanisms to ensure that it adheres to the originally proposed cost to the maximum extent possible.
* **Risk Management:** In furtherance of the cost control objective, <AGENCY> seeks to manage all contract risk, both in terms of project delivery and overall contract management. Such risks may include technical/operational risks regarding Operations and Maintenance (O&M) services; delivery/schedule risks related to all projects; and cost risks associated with overall program and individual project costs.

# Task 2 – Program Management Office (PMO) Services

The <AGENCY> CIO Program Management Office (PMO) is responsible for the successful introduction, integration, and maintenance of technologies which support <AGENCY> strategic goals, as well as the deployment and management of the services needed to empower staff to perform the mission of the Commission. The ever-growing need to adopt technologies to improve efficiency, effectiveness, agility, and durability requires the utmost diligence when <AGENCY> selects its IT investments.

The PMO incorporates management and administrative activities which integrate execution of tasks and projects managed by the <AGENCY> CIO. The PMO ensures that IT support across all tasks is conducted in a disciplined, well-managed, and consistent manner, and that quality solutions are delivered on time and within budget. The PMO employs proven project management best practices in order to achieve IT portfolio performance that operates within cost, schedule, and performance goals set forth for functional areas, operational tasks and projects.

The Contactor shall develop a means of aligning the PMO function to the Commission’s organization in a manner that supports PMO requirements presented below.

The PMO Support task provides two major support areas to the <AGENCY>:

1. PMO Services – PMO provides integrated management, disciplined execution, and reporting services on all efforts under the purview of the <AGENCY> CIO. In addition, the PMO executes a Continual Service Improvement (CSI) program across all IT functional areas and projects.
2. Technology Architecture Services – Technology Architecture Services set direction for the future technology framework in a manner which meets Commissions requirements to comply with evolving business needs, mandated federal policies and security directives while incorporating industry methods and best practices. Technology Architecture Services includes action required to analyze new and developing technologies for applicability to the <AGENCY>.

The Contractor shall provide PMO support functions for all projects and activities under the purview of the <AGENCY> CIO regardless of whether the activity itself is performed by the Contractor, federal staff or other organizations supporting <AGENCY>.

## PMO Services

The main purpose of the PMO support function is to integrate execution of all CIO efforts (operations and projects) using a proven, common project and program management framework. <AGENCY> expects that application of such commonality will enable the PMO to do the following:

* Successfully manage and coordinate efforts among operational and project activities,
* Integrate performance and execution data into actionable reports, and
* Execute a meaningful Continual Service Improvement (CSI) process.

Specific requirements are presented below.

### Program/Project/Task Coordination

The Contractor shall leverage program management industry best practices, establish project performance management, provide governance to process integration, and improve IT project productivity and product quality. Unless otherwise directed by the Government, all initiatives that are classified as projects shall be guided by a Project Management Plan (PMP) and shall undergo a disciplined monitoring and controlling process for tracking, reviewing, and regulating the progress to meet the performance objectives defined in the PMP.

The Contractor shall maintain detailed Project Management Plans for all ongoing projects and activities. The Contractor shall update these plans in a manner that supports regular project activity reporting and the Capital Planning and Investment Process (CPIC) and System Development Lifecycle (SDLC) processes.

The Contractor shall maintain detailed Concept of Operations for all ongoing tasks and operations activities. The Contractor shall update these documents in response to any operational changes.

The Contractor shall develop and maintain a Master Integrated Project Plan (MIPP). This master plan shall contain critical path information about all on-going projects and tasks and their inter-relationships and deliverables. Every time a new requirement is presented, the Contractor shall evaluate its impact on the ongoing activities and develop information about the impact of this new project on-going activities and plans. Results of these efforts shall be directly applicable to the requirements of the CPIC.

The Contractor shall establish standards, tools, reporting, software and procedures for project management and operations management. In addition, the Contractor shall establish and maintain standard management and reporting templates needed by all projects and tasks.

The Contractor shall provide guidance in project management processes, tools and methodologies in a manner that is efficient, consistent, and standardized, leading to successful project conclusion.

### Reporting

The Contractor shall collect, review, and compare actual project and operational performance against Project Management Plans and performance measures and assess performance to determine whether any corrective or preventive actions are indicated; when applicable, the Contractor shall recommend the corrective or preventive actions necessary.

The Contractor shall maintain accurate performance information and the associated documentation concerning all activities under the purview of the CIO.

The Contractor shall provide information to <AGENCY> management, the CO, and the COR as specified to support status reporting, progress measurement, and forecasting. Variance analysis, earned value analysis, and forecast data shall be a part of the status reporting.

### Program Improvement

The Contractor shall implement and execute a CSI program which analyzes all aspects of the <AGENCY>’s IT operations and develops recommendations for improvements.

The Contractor shall provide continuous monitoring and improvement of all activities (O&M and projects) and provide <AGENCY>’s management team insight into any areas that may require special attention.

The Contractor shall compile data and lessons learned about ongoing and completed projects for use on future projects.

## Technology Architecture Services

The Contractor shall analyze <AGENCY> business process models combined with the use of industry methods and best practices, and develop Technology Bricks, Standards, and Patterns for <AGENCY> Technology Architecture (TA). The framework for the TA will be developed in conjunction with the CIO. This TA will be used to guide new IT implementation as well as modernization efforts both in the near-term and three (3) to five (5) years out. The TA shall provide guidance on all components of <AGENCY> technology.

The Contractor shall assist with the preparation of a <AGENCY> IT Strategic Plan, including specific activities aligned with Commission goals and objectives. The <AGENCY> IT Strategic Plan addresses how IT will be used to support the business needs and priorities of the Commission. Additionally, the <AGENCY> IT Strategic Planning process establishes performance measures and metrics consistent with goals and objectives set in the Commission’s Strategic Plan.

# Task 3 – IT Policy Services

<AGENCY> Information Technology Policy Division serves as the administrative arm of the <AGENCY> CIO. This division is charged with developing and maintaining the IT Framework for the Commission, including maintenance of the Enterprise Architecture (EA) and all governing policies and procedures.

ITP is responsible for providing advisory and implementation support in the development of policy and procedures encompassing all CIO program responsibilities; ensuring that the CIO and the Commission meet all Federal mandates and guidance related to IT; and coordinating the review and reporting of the Capital Planning and Investment Control (CPIC) process. Additionally, ITP is responsible for conducting quarterly audits of IT systems, coordination of development and reporting of quantifiable performance measures for IT investments and providing processes to assess the investment’s value in achieving the Commission’s business plan.

ITP is the driving force behind the <AGENCY> Knowledge Management program. The program aims to optimize personal and organizational performance by encouraging, facilitating, and embedding practical collaboration and knowledge sharing strategies into the Commission's daily business operations.

## Enterprise Architecture Services Support

### EA Data Integrity

The Contractor shall maintain accuracy and completeness of the EA information (stored in TROUX system) about <AGENCY> assets and their relationship to each other and business needs. The Contractor shall perform a quarterly audit of existing EA information. To support these audits, the Contractor shall use procurement and security/asset scan information to verify and update information stored in the TROUX system. The Contractor shall investigate and resolve any discrepancies, including physical inventory, if required.

The Contractor shall develop and maintain a Commission Enterprise Data Inventory in accordance with the OMB’s Open Data Policy (M- 13-13).

### Enterprise Assets Lifecycle Support

The Contractor shall maintain current information about lifecycle of hardware and software system used by the <AGENCY>. The Contractor shall notify the CIO about any systems which are approaching end-of-life or end-of-support and develop mitigation strategies. The Contractor shall present quarterly reports about status of support for all <AGENCY> IT assets.

### Additional EA Support

The Contractor shall support the workings of the Enterprise Architecture Working Group (EAWG). The EAWG is a governing body which sets the direction and makes adjustments to the exiting EA baseline. To support the EAWG, the Contractor shall:

* Provide technical and business inputs regarding decisions before the Group.
* Ensure adherence of projects conformance to the baseline architecture.
* Perform Impact Analysis (IA) for all Change Requests (CRs).
* Provide architecture information and recommendations to implementation teams.

The Contractor shall maintain the <AGENCY> Enterprise Roadmap document. This document uses the Common Approach to Federal Enterprise Architecture to map the organization’s strategic goals to business services and the integrating technological solutions across the enterprise. It identifies performance gaps, resource requirements, planned solutions, transition plans and summarizes the current and future architecture. It describes the EA governance process and implementation methodology.

The contractor shall also assist the CIO in the development and maintenance of the CIO Service Catalog. Additionally, the Contractor shall support the CIO in preparing the overall IT portfolio, inclusive of both major and non-major IT initiatives, for submission to the OMB.

The Contractor shall address data requests made in response to the Commission’s annual FISMA audit.

## Capital Planning and Investment Control (CPIC) Services

<AGENCY> CPIC and OMB Budget Submission processes, tailored for a small agency, are well-established repeatable processes in which IT initiatives are selected, prioritized, and then continually monitored and evaluated to ensure each chosen initiative is well managed, cost effective, and supports the mission and strategic goals of the Commission. <AGENCY> CPIC process is an integrated, structured methodology to managing IT investments, which ensures that such investments align with <AGENCY> mission and support business needs while minimizing risks and maximizing returns throughout the investment’s lifecycle.

To support <AGENCY> CPIC process, the Contractor shall:

* Maintain the policies, procedures, and the SharePoint CPIC portal associated with the CPIC program.
* Develop business cases, ensuring that they are well-documented, complete, and contain accurate cost and technical requirements, that enable the CPIC Control Board to make fully informed decisions about proposed investments. The Contractor shall work with the <AGENCY> business units to complete CPIC-required documentation.
* Conduct periodic audits of software and programs which were approved and implemented through the CPIC process to support analysis regarding initiatives’ success and need for future maintenance. To support these efforts, the Contractor shall develop reports, which include Return on Investment (ROI) and information about the project’s ability to provide the anticipated benefits. The Contractor shall follow the <AGENCY> CPIC Evaluation process.
* The Contractor shall maintain all business documents related to CPIC within <AGENCY> CPIC SharePoint portal.

## Knowledge Management Services

<AGENCY> employees and contractors include attorneys, judges, accountants, engineers, economists, rate analysts, etc. In the current work environment, <AGENCY> personnel, both government employees and contractors, often work on isolated activities, spread across the various regional offices throughout the country. A large number of current <AGENCY> practices are undocumented, while documentation for other processes is outdated and in need of revisions. Furthermore, with a number of essential personnel nearing retirement, preserving and maintaining institutional knowledge, tricks of trade, and other intangible assets is of paramount importance. Currently, a percentage of full-time personnel are eligible for retirement. When these individuals leave the Commission, there is concern that they will take decades of institutional knowledge with them.

<AGENCY> has implemented a Knowledge Management Program in an effort to mitigate the loss of institutional and industry, tangible and intangible knowledge lost through attrition. The Contractor shall support <AGENCY>’s Knowledge Management Project in order to capture and centralize the knowledge and documentation of <AGENCY> policies, procedures and soft work “tricks” into a SharePoint platform that will permit staff to access this information. The current approach to gathering this information is for the ITS support Contractor to conduct the initial knowledge gathering, train the KM Leader (Federal employee) and turn over continuous information gathering and classification process to the individual <AGENCY> organizations.

To support the KM requirements, the Contractor shall conduct two Knowledge Management Assessments each quarter. To support these assessments, the Contractor shall:

* Develop marketing and communication plan and promote the KM services throughout <AGENCY>.
* Maintain the KM Service Catalog with accurate information on all KM services provided by the Commission.
* Conduct knowledge assessment interviews with program staff and management and document findings.
* Conduct training for personnel designated to become Knowledge Leaders, or other interested <AGENCY> employees.
* Create, maintain and update associated training materials.
* Create computer base training courses for KM Leaders and publish on <AGENCY>’s intranet.
* At the completion of all assessments, meet with the government to review preliminary findings and outline the KM catalog services that should be implemented with an implementation timeline.
* Solicit feedback through a customer satisfaction surveys to obtain user input, measure and track customer satisfaction, and take steps to ensure that overall satisfaction with the KM program remains high.
* The Contractor shall maintain all business documents related to KM within the <AGENCY> KM SharePoint portal.

## Regulatory Compliance Support Services

White House, OMB, and the Federal CIO are responsible for providing oversight on how agencies devise, implement, manage, and evaluate the statutory programs and policies for which they are responsible. Often, mandates will impact the <AGENCY> CIO’s areas of responsibility. The Regulatory Compliance Support Services ensures that <AGENCY> is aware of and responds appropriately to these mandates.

To support these services, the Contractor shall:

* Ensure that the CIO remains in compliance with all IT Federal mandates. This includes identifying, tracking and responding to IT related Executive Orders, Presidential Memorandums, OMB Circulars, Acts and other guidance released by the White House, OMB and the Federal CIO.
* Proactively monitor requests from OMB, NIST and other requests for federal compliance on IT systems that may have an impact on CIO areas of responsibility and ensure that the CIO is aware of the mandates, requirements, due dates, and impact on the Commission.
* Manage lifecycle of IT Federal mandate requirements from receipt of request, gathering supporting documentation, drafting response and submission of compliance documentation.
* Maintain compliance information in the SharePoint-based CIO Mandates Dashboard.
* Provide an audit which assesses adherence of the <AGENCY> operations against the lifecycle of OMB mandates as required by the government.

## IT Policy Documentation Services

<AGENCY> IT policies and procedures and other governance documents need to be created and updated on a regular basis. The Contractor shall develop new IT-related governance documentation and validate and update existing documentation as described in <AGENCY>’s *CIO Policy and Standard Operating Procedures* governance. Successful execution of tasks listed below requires experience with developing IT policy and cross functional knowledge of <AGENCY>’s OMB compliance and CPIC processes.

Specifically, the Contractor shall:

* Develop and/or update IT related governance documents including Policy, Standard Operating Procedure (SOP), Charters, Guides, Catalogs, and other governance documents as the government deems necessary. Review the current policies and procedures, guides, and other governance documents for changes.
* Maintain the information in the SharePoint-based CIO Policy Dashboard, which tracks all CIO policies.
* Develop training materials and conduct classes to provide training on new policies to <AGENCY> personnel and stakeholders.

# Task 4 – Operational Support

The <AGENCY> is responsible for maintaining delivery of all IT support services to IT users. The objective of the division is to integrate new technology that effectively supports <AGENCY>’s business demands in a cost-effective manner and maintain a stable and secure IT environment that protects and presents the information that facilitates <AGENCY>'s mission. <AGENCY> is focused on providing <AGENCY> customers with quality, timely and cost-efficient maintenance, modernization, and technical support provided in the IT Service Catalog (EAL). The scope of this task includes all facets of operations for computer, network, communications, and hardware and software infrastructure technologies. The primary objectives of the <AGENCY> task areas are to provide continuing IT services integration and technical support to <AGENCY> with an emphasis on customer service to meeting mission requirements. The <AGENCY> Task consists of 4 major areas of support:

* IT Customer Support Services – IT Customer Support Services include the IT Service Desk (SD) (Tier 1 user support) and hands-on support (Tier 2 functions). The IT Service Desk seeks to provide the user with an informed single point of contact support for all IT functions. Tier 2 provides user-centric support including user hardware and software delivery, installation, and break-fix support. Account management ensures currency and accuracy of all user and computer accounts.
* Infrastructure Support Services – Infrastructure Support Services consists of a number of programs that provide operational and maintenance support to all facets of the network infrastructure. The scope consists of the Tier 3 operational support of System Administration, Storage Area Network, Network Attached Storage, Local Area Network, Wide Area Network, IT System Monitoring, Web Services, Messaging, Business Continuity, and Disaster Recovery. This area includes support services for systems located at <AGENCY> and cloud services. In addition, this area includes the Account Management Services provide ongoing management of all user, machine and service accounts. This service also manages types and number of licenses.
* COOP Services – COOP Services ensure that the <AGENCY> COOP site is ready to assume operational responsibility in case of full or partial loss of functionality of systems operating at the <AGENCY> HQ.
* Training Support Services – Training Support Services develops and conducts User training for various <AGENCY> IT-related applications and systems.
* See ATTACHMENT NN for a definition of the ITS Service Desk and Operational Support Tiers.

## IT Customer Support Services

The objective of this service is to ensure that <AGENCY> users receive effective customer-centric support of IT requests, and to resolve technology issues in an expedient manner. <AGENCY> currently achieves this through the use of a tiered, Information Technology Service Management (ITSM) based service delivery model; Tier 1 (IT Service Desk) and Tier 2 (hands-on support). To maintain a high level of user satisfaction, <AGENCY> expects that the Contractor be able to resolve a majority of issues during the initial engagement with Users. <AGENCY> standardized on the Information Technology Information Library (ITIL) as the standard for its IT operations.

The Contractor shall “own” the resolution process from the initial contact with the User to resolution of the Incident, Problem or Service Request. The Contractor shall assume responsibility for Incident, Problem and Service Request resolution regardless of the party actually performing the work, i.e., if the work is performed by an organization external to the Service Desk (SD), the SD is still responsible for tracking and documenting the resolution process. The SD shall escalate tickets, as required by the SLAs. As with any IT operations, changes to operations should be expected. As such, the Contractor shall support project associated with making incremental changes to the operational artifacts in response to governance, industry or customer requirements.

Although fluctuating somewhat, the recent ticket volume was approximately 40,000. <AGENCY> does not have call statistics.

### Overarching Requirements

The Contractor shall:

* Follow-up on resolved tickets to check quality, get User concurrence of ticket closure, and to report customer satisfaction.
* Work with Operational and other teams to ensure final summary, review, analysis, resolution, and lessons learned are documented in Incident Reports for all major Incidents and unplanned service outages, and submitted in writing to <AGENCY> management and the COR.
* Establish and maintain data in the <AGENCY> Known Error Database; document workarounds and generate known error sub-processes to facilitate quicker diagnosis and resolution for future Incidents.
* Proactively monitor Service Desk calls, Incidents and Service Request work flows, processes and queues to immediately identify and address performance issues that will impact the delivery of services to Users.
* Ensure non-IT requests are properly routed to appropriate support organizations.
* Contractor shall support projects associated with making changes to the operational artifacts in response to governance, industry or customer requirements.
* Provide operational reports and support the program-wide continual service improvement (CSI) initiatives (please see the Program Management Office Support section for details).

### Tier 1 Support

#### Hours of Support

The Contractor shall provide live SD services during the Normal Support Hours (NSH) of 0700 through 1800 ET Monday through Friday, excluding Federal holidays. All calls, emails, faxes, etc. received outside the NSH shall be addressed during the first hours of the next business day’s NSH.

#### Initial Ticket Handling

The Contractor shall provide live Tier 1 SD support during NSH. The SD shall accept Users' requests for service (regardless of a communication method), record the request, and attempt resolution. If the agent handling the request cannot resolve the issue, the Contractor shall escalate the ticket to the appropriate personnel. To properly handle incoming calls, the Contractor shall:

* Provide live telephone coverage during normal support hours.
* Answer customer telephone calls and emails to the SD in accordance with the applicable SLAs during normal support hours (see ATTACHMENT J-2).
* Monitor voicemails, emails, fax, and Web requests for service requests.
* Record any additional information obtained from the User in the ITSM system.
* Assign ticket priority based on the applicable SOP.
* Provide the User with a ticket number.
* Perform initial diagnosis and analysis of Incidents and provide immediate resolution and recovery if possible.
* Use remote control tools to assist and resolve customer incidents.
* Provide warm handoff escalation of incidents that cannot be addressed by the initial contact.

#### Ticket Updates

The Contractor shall update or ensure that all tickets are updated in a manner that meets the applicable SLAs. To properly manage tickets created by or assigned to the Contractor, the Contractor shall:

* Update tickets by adding work log information as required by the applicable SLAs.
* Monitor status of all open tickets and escalate as required or dictated by the SLAs.
* Coordinate resolution with other internal and external teams, as appropriate.
* Provide advice and guidance to the Users regarding restoration of interrupted service.
* Provide advice and guidance to Users regarding restoration of interrupted service.

#### Ticket Closure

<AGENCY> requires that no ticket be closed without concurrence from the User that the issue represented by the ticket has been fully resolved and that the service has been restored. The Contractor shall verify ticket closure with the requester.

#### Outage Communication

<AGENCY> uses a combination of notification tools, including email and postings on internal and external Web sites to make users aware of any issues which have a negative effect on IT service delivery. The Contractor shall communicate system outages in accordance with established SOP to appropriate <AGENCY> points of contacts and end users using <AGENCY>-provided tools and communication methods and continue ongoing communications until the Incident/Problem has been resolved and all services have been restored. Contractor shall be responsible for managing content of the notification messages. All new messages or updates to the existing massages must be approved by the Federal IT Operations Point of Contact prior to posting.

### Tier 2 On-site support

The Contractor shall provide a full range of hands-on IT-related support functions at <AGENCY>-designated locations (see section below).

#### Hours of Support

The Contractor shall provide dedicated on-site support at the HQ facility in XXX during the hours of 0700 through 1800 ET Monday through Friday, excluding Federal holidays.

#### Locations Requiring On-Site Support and Hours of Operations

Contractor shall provide dedicated on-site support to the <AGENCY> headquarters facility located in XXX. All other facilities listed below do not require a dedicated staff; rather the Contractor may be required to travel to these sites on as needed basis. The table below presents approximate number of staff (at time of this writing) requiring support. Number of staff can fluctuate depending on time of year, but the upper bound of users is anticipated to be 1,700.

#### On-Site Support Requirements

The Contractor shall be responsible for on-site support of computing devices (desktops, laptops, handheld devices, printers, etc.) and associated software at the locations listed above. To support these, the Contractor shall:

* Configure, install, and troubleshoot <AGENCY>-approved laptops, desktops, printers, network- connected copiers, scanners, and other office IT equipment.
* Configure, install, and troubleshoot <AGENCY>-approved software elements including the operating system (OS).
* Maintain and upgrade software elements, including the OS.
* Move existing devices within a single office building.
* Troubleshoot software and hardware issues.
* Troubleshoot configuration problems.
* Assist Users with application usage questions and concerns.
* Escalate hardware repair/replacement issues to <AGENCY>-contracted hardware vendors, if applicable.

Please note that most of the support functions for locations other than the HQ can (and currently are being) performed remotely with very limited need to travel outside of the HQ facility.

### Walk-In Center at the <AGENCY> HQ

The Contractor shall operate the existing Walk-In Center at the <AGENCY> HQ Building. The purpose of this center is to provide Users with a central place where they can drop off, pick up equipment, and pick up Service Request forms. The Contractor shall ensure that the walk-in center is staffed during the NSH.

## Infrastructure Support Services

The objective of this service is to effectively manage the <AGENCY> infrastructure and catalog of services in order to provide maximum stability, availability, security, and reliability. The Contractor shall provide services listed below to all <AGENCY> locations listed above.

### Hours of Support

The Contractor shall provide live Infrastructure Support services during the Normal Support Hours (NSH) of 0700 through 1800 ET Monday through Friday, excluding Federal holidays.

### Data Communication and Internet Access Support

<AGENCY> uses services of a Network supplier to provide network connectivity among its facility. In addition, <AGENCY> uses services of an Internet Service Provider to secure internet access to all <AGENCY> sites. In general, the service providers’ responsibility ends with their edge router located at a <AGENCY> facility. <AGENCY> manages data routing within and out of their facilities.

The Contractor shall:

* Monitor all network management systems and respond to all network alerts in a manner required by the applicable SLAs.
* Isolate and resolve network faults.
* Maintain, upgrade, and troubleshoot all <AGENCY>-owned network elements:
  + Routers
  + Hubs
  + Switches
  + Security
  + Domain Controllers
  + Security devices
* Maintain access to the Internet.
* Maintain and manage IP address range configurations.
* Work with the network telecommunications service providers in resolving service problems.
* Monitor network telecom service provider’s SLAs and work with the providers to resolve issues and provide credits.
* Work with the local staff in resolving data communication problems.
* Monitor circuit utilization and (upon approval) manage bandwidth upgrades/reduction as required.
* Develop and maintain site-specific equipment inventory and configuration. The site-specific information shall include:
  + “As-built” diagrams and schematics
  + Rack space layouts
  + Equipment interconnectivity
* Maintain telecom circuit inventory, including address and configuration information for the Service Delivery Point (SDP), DMARC and Extended DMARC, LEC circuit IDs and other pertinent information for all circuits managed or used by the <AGENCY>.

### Classroom and Conference Room Support

<AGENCY> has separate support contracts for audio, video, and display systems deployed at conference rooms and a classroom located at the HQ. The Contractor shall accept initial requests for service and coordinate with the external support contractor to resolve the issue.

### Video Conference Support

<AGENCY> uses video services extensively to provide video communications with the public and to coordinate internal efforts.

To support the video operations, the Contractor shall:

* Coordinate video conferences.
* Support daily video operations.
* Troubleshoot connectivity and configuration issues.
* Conduct direct support of video conference equipment.

### Server Systems

The Contractor shall provide O&M service of the servers supporting <AGENCY> operations. The approximate numbers and types of servers are presented in ATTACHMENT J-3 Environmental Asset Library (EAL).

### Authentication Services

The Contractor shall assume responsibility for planning, updates, and O&M of the <AGENCY> authentication services structure.

To support these requirements, the Contractor shall:

* Manage all objects within the authentication service structure (policy, user, computer, groups). The current count is approximately 87,000 objects.
* Maintain authentication services root and local level structures, as required.
* Maintain and update:
* Domain plan and design documentation
* Organization Unit (OU) plan
* Enterprise Group Policy
* Manage local-level domains.
* Manage site replication.
* Manage security patches and antivirus signatures on <AGENCY> domain controllers.
* Perform troubleshooting of the Domain Name Services (DNS).

### Email Services Support

The <AGENCY> is using a cloud-based email solution to provide standard email and calendar collaboration functionality to its users. To maintain proper functionality of this email solution, the Contractor shall:

* Manage (create, modify, delete, and set permissions) mailboxes and folders, both private and public.
* Manage (create, modify, and delete) email address groups.
* Create, delete, and set permissions on private and public mailboxes and folders.
* Add/delete users to/from public folders.
* Create, alter, and remove distribution lists.
* Coordinate resolution of issues with the email service provider.

### Equipment Support

The <AGENCY> CIO is responsible for tracking and deployment of all IT equipment to all <AGENCY> locations. The actual process of deployment varies base the underlying contractual agreements <AGENCY> has with the equipment supplier; some equipment is shipped to the <AGENCY> HQ for processing and shipment to the sites, some arrives directly at the final destination. Regardless of the shipping method, the Contractor shall support the following activities:

* Break Fix Support:
* Order the appropriate replacement parts.
* Configure as required.
* Ship to site.
* Perform on-site installation, including scheduling with site personnel.
* Dispose of the broken equipment.
* Support for new equipment:
* Work with the <AGENCY> leadership to identify required configuration.
* Assist with ordering.
* Accept equipment form the vendor.
* Deploy new equipment.
* Remove and dispose of the old items.

The Contractor shall be responsible for making updates to the asset and configuration databases as equipment is retired, new is put into operations, or any other changes are made.

Please refer to ATTACHMENT J-3 Environmental Asset Library (EAL) for list of equipment which needs support.

### Web Services and Share Point Support

The <AGENCY> provides hosting of existing and development of new <AGENCY> web sites primarily using Window’s SharePoint service suite. The Contractor shall:

* Develop new and update/replace existing web and SharePoint content. The Contractor shall obtain approval from <AGENCY> prior to making any changes.
* Manage and maintain uniform “look and feel” of all managed web sites. <AGENCY>-managed Web pages include:
* Insert list
* Manage SharePoint hosting environment, including:
* SharePoint software and its updates.
* Maintain databases and its content (SQL).
* Maintain security and access:
* Maintain permission groups.
* Maintain existing and create new access accounts.
* Assist SD with troubleshooting.
* Develop scripts to enhance ease of access to information, as required.

### ITSM System Support

The Contractor shall provide ongoing O&M support of the <AGENCY>’s ITSM v.8 system, which consists of Service Desk, Change Management, and Asset management modules. To provide this support, the Contractor shall:

* Maintain operational readiness of the ITSM server software, Web interface, and associated SQL databases.
* Manage appropriate numbers and types of user licenses.
* Implement workflow changes as required by changing environment.
* Update data selection.
* Assist with automating reports.
* Maintain user accounts.
* Perform standard administrative system configuration (such as add location, groups, etc.)

### Enterprise System Backup and Restore

The Contractor shall perform ongoing backup (daily, weekly, monthly) of data stored in primary systems (at <AGENCY> HQ) to the COOP location, including, but not limited to:

* Active Directory elements
* Network monitoring and other NOSC tool servers
* ITSM
* CMDB
* File system data (both structured and unstructured)

### Enterprise Management Systems

The Contractor shall be responsible for operating, configuring, and managing <AGENCY> system management (GFE) including:

* Microsoft System Center Operations Manager (SCOM)
* Microsoft System Center Configuration Manager/SMS (SCCM)
* SolarWinds Orion
* BMC ProactiveNet

### O&M Support of the HQ Data Center Infrastructure

The Contractor shall perform O&M for the <AGENCY> data center located at the <AGENCY> HQ. The Contractor shall support and perform hardware/software O&M, System Administration, Capacity Management, Configuration Management, Backup and Recovery, IT Systems Monitoring, and continuous optimizations for the following operational environments:

* Data Storage
* Storage Area Network
* Network Attached Storage
* Virtualization
* UCS
* Business Application Support
* Cloud Services Support
* Web Services Support

In addition, the Contractor shall assume responsibility for managing and adjusting in size as required the physical infrastructure of the data center, including (but not limited to) racks, UPS, data communication (LAN), power, and HVAC.

### O&M Support of the Local IT Infrastructure

The Contractor shall provide remote O&M of the LAN and the associated systems at all <AGENCY> locations, including performance, security monitoring, and configuration changes.

### Business Content Management

The Contractor shall manage and maintain the creation of <AGENCY> business content for both <AGENCY>’s Internet and Intranet presence.

### IT Assets Management (ITAM) Program Support

<AGENCY> uses a comprehensive set of tools and systems to maintain up-to-date information about its assets and their configuration. The Contractor shall maintain accuracy of this information by updating asset and configuration information within 12 hours of any change to the actual asset.

### Support of the Business Center Support

The Business Center is a shared office space which contains laptops, printers, plotters, scanners, and other office system. The Business Center is available to authorized users, both internal and external. The Contractor shall provide O&M services for all of the equipment in the Business Center.

### Telephone Systems Support

The Contractor shall provide O&M support of the telephone systems deployed at <AGENCY> locations. <AGENCY> has approximately XXX Cisco Unified IP Phone 7945 and XXX of Cisco’s 7965 sets.

### Account and License Management Services

The Contractor shall be responsible for accepting initial paperwork and assisting <AGENCY> with obtaining approvals as well as creating new or making changes to existing accounts (user, service, and machine). In addition, the Contractor shall monitor usage of licensed software to ensure that <AGENCY> has the appropriate amount and type of licenses.

### Secure Vault Support

<AGENCY> maintains a small Top-Secret (TS) Sensitive Compartmented Information Facility (Secure Vault) at the HQ building. This Secure Vault contains less than ten (10) workstations and the associated communication equipment.

The Contractor shall provide the same level of O&M services and support to the equipment in this Secure Vault required for the rest of <AGENCY> computer equipment.

The Contractor shall ensure that the personnel assigned to performing any duties in the Secure Vault have a Top-Secret security clearance.

## COOP Operations

<AGENCY> hosts its COOP system in Germantown, MD. The COOP site contains systems required to operate and manage <AGENCY>’s computing infrastructure but does not contain space for staff. The systems at the COOP site need configuration which mirrors that of their production counterparts. To support COOP operations, the Contractor shall:

* Ensure that all the equipment at the COOP site is configured identical to the analogous equipment at the <AGENCY> HQ.
* Ensure that all systems within the COOP facility are ready to take over operations from the systems located at the primary location within one (1) hour of the primary system‘s failure or time designated and validated by government review within the contractors.
* Ensure that the COOP systems are:
* Built with the same software release levels and patches as the primary systems.
* Configured with the same configuration information as the primary systems.
* Capable of operating on their own in case of partial or full failure of the primary systems.
* Maintain Continuity of Operations Plan (COOP) to reflect any changes in the operational environment.
* Support a yearly Eagle Horizon exercise.
* Support two (2) full and two (2) partial <AGENCY>-initiated Disaster Recovery (DR) exercises per year.

## Training Support

The Contractor shall provide support and maintain a scalable training program to enhance the skills of the <AGENCY> workforce as it relates to the use of IT software and hardware associated with the <AGENCY>'s current and future computing environments. <AGENCY> has a current training program, which provides on-line and classroom training to its Users. The Contractor shall provide a full range of support of the training program, including but not limited to development of training materials, both on-line and classroom, schedule and conduct classes as well as seeking and reporting on feedback from the students regarding quality of the training. Currently, all classroom classes are held at the <AGENCY> HQ.

# Task 5 – Information Security and Systems Assurance (ISSA) Services

ISSA provides the <AGENCY> with security services that minimize exposure to threats, mitigate risks, protect assets and privacy information, and maintain configuration management.

The Federal Information Security Management Act (FISMA) was passed in 2002 and requires every Government Agency to secure the information and information systems that support its operations and assets, including those provided or managed by another Agency, Contractor, or other source.

The core ISSA functional task areas include:

**Network Security Management** – Ensure security awareness, risk management, and effective Incident Handling and Response to network and information security incidents.

**Security Compliance and Reporting** – Ensure compliance with FISMA, NIST security guidelines, and OMB mandates.

**Configuration Management** – Ensure consistency through the collection of processes and tools, track changes, and provide up-to-date documentation, in a centralized configuration management program.

**Assessment and Authorization (A&A)** – Support ongoing A&A and C&A activities.

**Information Security Continuous Monitoring (ISCM)** – Support implementation of Continuous Asset Evaluation Situational Awareness and Risk Scoring (CAESARS).

**Systems Assurance** – Ensure products and services are defect-free through Systems Acceptance Testing (SAT).

**Records Management Support** – Ensure adequate and proper documentation for all filings and issuances is maintained throughout the record life-cycle, and disposition records as required by the National Archives and Records Administration.

## Network Security Management Services

The objective of this task area is to implement a network security management framework that consists of:

1. Prevention
2. Continuous Monitoring
3. Detection
4. Containment
5. Eradication
6. Recovery
7. Follow-up

Network Security Management serves as an umbrella of the processes that ensure security awareness, risk management, effective incident handling and response to network threats, and information security incidents targeting enterprise assets. Critical success factors include personnel with the appropriate skill sets, defined and adaptive processes, and leading- edge technologies.

The requirements for this service area are:

The Contractor shall monitor security trends and perform feasibility studies for the implementation of new security technologies that best meet the Commission’s business needs and meet cost, performance, and quality objectives.

The Contractor shall provide annual audits (or as required by FISMA) of the architecture and configuration of <AGENCY> key cybersecurity infrastructure including firewalls, intrusion detection systems, content filtering/monitoring, vulnerability assessment tools, file integrity monitoring, centralized audit log store, and other network/system monitoring tools.

The Contractor shall provide short and long-term risk assessments of integrating new technologies and processes as they relate to Confidentiality, Integrity, and Availability (CIA).

The Contractor shall perform vulnerability assessments and scans of the <AGENCY> infrastructure, as required per <AGENCY> policy (*<AGENCY>\_VMP\_Final* in the EAL) and ensure vulnerabilities and weaknesses are identified and mitigated.

The contractor shall support security related data calls or investigations.

The contractor shall administer Intrusion Prevention System (IPS).

The Contractor shall respond to and report all incidents concerning intrusion and virus infections.

The Contractor shall create and update firewall rules to accommodate access to appropriate data sources.

The Contractor shall test new tools and patches prior to deployment.

The Contractor shall manage security patches and antivirus signatures and apply security patches in accordance with <AGENCY> policy *(note that <AGENCY> may not require this support for the full order period of performance)*.

The Contractor shall eliminate unauthorized traffic traversing the network as identified by the <AGENCY>.

The Contractor shall provide immediate support to serious incidents, intrusions or comprises (classified spillage, unauthorized intrusion, or virus outbreak).

The Contractor shall provide computer/network incident response capabilities to detect, analyze, and propose responses to security incidents.

The Contractor shall collect and analyze network intrusion artifacts from a variety of sources to include logs, system images, and packet captures to enable mitigation of network incidents.

The Contractor shall perform network analysis (including wireless) to look for unauthorized devices. SolarWinds is the current tool maintaining the event management log.

The Contractor shall implement a security vulnerability tracking methodology.

The Contractor shall record and respond to all security incidents. A security incident is the act of violating an explicit or implied security policy. These include but are not limited to:

1. Attempts (either failed or successful) to gain unauthorized access to a system or its data
2. Unwanted disruption or denial of service
3. The unauthorized use of a system for the processing or storage of data
4. Changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent.

The Contractor shall create or manage the existing Plan of Actions and Milestones (POA&Ms), as required to maintain FISMA compliance.

The Contractor shall ensure all IT infrastructure changes adhere to cyber security policies and recommend remedial actions, in accordance with Federal and <AGENCY> policies and procedures.

The Contractor shall analyze all bulletins provided by US Computer Emergency Readiness Team (CERT), Joint Cybersecurity Coordination Center (JC3), GSA’s Managed Trusted Internet Protocol Service (MTIPS) providers, Office of Management and Budget A-130, NIST Special Publications, and any other sources applicable to <AGENCY>, and provide mitigation plans to ensure timely remediation.

## Security Compliance and Reporting Services

The Contractor shall ensure security compliance by adhering to the Federal Information Security Management ACT of 2002 (FISMA) and National Institute of Standards and Technology (NIST) security guidelines, and other Office of Management & Budget (OMB) mandates. FIPS Publication 199 defines three (3) levels of potential impact on organizations or individuals should there be a breach of security (i.e., a loss of confidentiality, integrity, or availability), which are used to categorize IT systems.

Currently, <AGENCY> has four (4) systems with FIPS 199 “moderate” categorizations. These are: <AGENCY> Annual Charges System (FACS), General Support System (GSS), <AGENCY> OnLine (FOL), and eLibrary. These systems are documented in the Environmental Asset Library (EAL). The Authority to Operate (ATO) expiration dates are as follows:

Table 1 – Major System Authority to Operate Expiration

| <AGENCY> Major System | ATO Expiration |
| --- | --- |
| <input text here> | <input text here> |
| <input text here> | <input text here> |
| <input text here> | <input text here> |

<AGENCY> is required to perform an annual independent evaluation of its information security program and practices to determine its overall effectiveness.

The requirements for this service area are:

The Contractor shall support the annual FISMA audit by responding to auditors’ data calls; confirming security controls; assisting with testing control effectiveness; identifying control deficiencies; and reporting findings to <AGENCY> management and staff.

The Contractor shall maintain a record of accreditations and ATO expiration dates, and report monthly on upcoming expiration of accreditations within a six (6)-month time horizon.

The Contractor shall maintain the <AGENCY> FISMA Plan of Action and Milestones (POA&M), including action items identified from all external and internal audits and all internal risk assessments and other activities.

The Contractor shall provide ad-hoc support such as preparing responses to OMB information requests, data calls, and requests from other entities as required.

The Contractor shall conduct a pre-audit assessment which includes reviewing prior year FISMA audit issues; updating documentation frequently requested; and conducting “pre-audit” of commonly audited areas and identifying weaknesses. The “pre-audit” activities shall be conducted three (3) months prior to audit.

The Contractor shall support the major systems security re-accreditation every three (3) years.

The Contractor shall maintain the Office of Inspector General (OIG) Notification of Findings and Recommendations (NFR) list, including action items identified from all external and internal audits, all internal risk assessments, and other activities.

## Configuration Management Services

Configuration Management (CM) is the process of identifying all components and their relationships in a continually evolving system, taking into account relevant system interfaces, for the purpose of maintaining integrity, traceability, and control over change throughout the lifecycle.

It is a disciplined process of technical and administrative direction for the identification and documentation of a system’s functional and physical design requirements; the management of subsequent changes; and the verification of successful requirement implementation.

<AGENCY> is continuously trying to align with evolving IT industry best practices, the changing application of IT in the workplace, and Federal mandates. The Contractor shall provide Configuration Management support services, including the collection of processes and tools that promote consistency, track and control change, and provide up-to-date documentation.

The requirements for this service area are:

The Contractor shall execute all approved <AGENCY> Configuration Management (Plans, Policies, and Standard Operating Procedures (SOPs) and update in accordance with FISMA, OMB, and NIST guidance.

The Contractor shall initiate, control, track, and audit changes, deviations, and waivers to CM processes according to current <AGENCY> approved processes.

The Contractor shall maintain a Configuration Management Database (CMDB), which is a central repository of hardware and software configuration items. The CMDB currently resides in SharePoint, DevTrack and VSS. Asset Management is provided by Troux and Sunflower.

The Contractor shall migrate software builds from development environment into test and production environments.

The Contractor shall manage the <AGENCY> Configuration Change Notification (CCN) Process for implementing changes.

The Contractor shall monitor and audit configuration changes to hardware and software to confirm that configuration management records and configuration items are complete, consistent, accurate, and ensure compliance with approved configuration baseline.

The Contractor shall ensure all implementations of IT investments or requests are in compliance with the <AGENCY> System Development Life Cycle (SDLC).

The Contractor shall perform ongoing reviews, analysis, and updates to all defined baseline configurations based upon federal hardening standards adopted by <AGENCY>.

## Ongoing Assessment and Authorization (A&A) Services

<AGENCY> seeks to augment the traditional C&A with an ongoing assessment and authorization process based on an Information Security Continuous Monitoring (ISCM) program that enables ongoing security authorizations of its major applications and general support systems.

The requirements for this service area are:

The Contractor shall provide their approach to maintaining independence of the verification process from the execution of traditional network security management services.

The Contractor shall develop ongoing assessment and authorization processes that are in compliance with the latest NIST SP 800 series, OMB guidance, and NIST/DHS current CONcept of OPerations (CONOPS) for Ongoing Assessment and Authorization.

The Contractor shall review <AGENCY> current C&A process and develop a strategy to align traditional C&A efforts into the current System Development Lifecycle (SDLC) and the Information Security Continuous Monitoring (ISCM) framework capability.

The Contractor shall support the C&A efforts as outlined in the SDLC to ensure FISMA compliance, including systems deployed in a Cloud computing environment supported by FedRAMP.

## Information Security Continuous Monitoring (ISCM) Services

The ISCM program supports ongoing assessment and authorization of information systems, as described in the latest NIST, OMB, DHS guidance, and implements ISCM tools and technologies using the CAESARS Technical Reference Architecture (Continuous Asset Evaluation Situational Awareness and Risk Scoring), and works in conjunction with <AGENCY> Continuous Diagnostic and Mitigation (CDM) program. These tools and technologies can enable and assist automated monitoring in support of a variety of <AGENCY> risk management processes such as continuous assessment of security control effectiveness, security status reporting of enterprise architecture and operating environment, assurance of compliance with internal and external security requirements, and analysis of security impact of changes to <AGENCY> live environment. The ISCM program’s goal is to also provide automated monthly data reporting of key metrics directly from security management tools to <AGENCY> CyberScope portal for FISMA reporting

The requirements for this service area are:

1. The Contractor shall assist <AGENCY> in developing a governance structure that utilizes the NIST CAESARS Technical Reference Architecture to implement technologies to automate ISCM activities in support of organizational risk management policy and strategy, operational security, internal and external compliance, reporting, and documentation needs.
2. The Contractor’s resulting governance structure shall work in conjunction with <AGENCY> Continuous Diagnostic and Mitigation (CDM) program and technologies.
3. The Contractor shall assist <AGENCY> in providing monthly data reporting to CyberScope; respond to security posture questions; and participate in <AGENCY>-led CyberStat review sessions and Commission interviews to develop actionable plans for improving <AGENCY>’s information security posture.
4. The Contractor shall build governance structure and automated processes to capture asset changes, configuration changes, and vulnerabilities using CVE/CVSS SCAP-based numerical risk values for the enterprise infrastructure assets with an automated vulnerability and risk analysis tool capability with a frequency of every 72 hours.
5. The Contractor shall prepare all technical, management, and operational documentation required, including project plans, to support each identified activity under the Information Security Continuous Monitoring (ISCM).
6. Systems Assurance Services
7. The Contractor shall systematically plan and conduct a set of quality control and assurance activities to assure systems engineering software fixes and enhancements conform to system requirements, are defect-free, and suitable to be deployed in the “live” environment. The Contractor shall conduct Systems Acceptance Testing (SAT) in order to provide an independent and objective evaluation of the operational effectiveness and suitability of systems deployed by <AGENCY>. SAT is intended to be an objective, thorough and realistic performance evaluation under real-world conditions.
8. <AGENCY> deploys major releases supported by a Project Management Plan (PMP) and full SDLC, and System Change Requests (SCRs) as needed. SCRs are typically bug-fixes or minor enhancements.
9. The requirements for this service area are:
10. The Contractor shall ensure that deliverables from the PMPs or SCRs meet required objectives by conducting systems assurance testing as determined by the project plan.
11. The Contractor shall ensure that projects will meet objectives for safety, security, reliability, quality, and functionality at the key points in the development process, (Design Reviews and Test Events).
12. The Contractor shall inspect projects for compliance with relevant standards as defined by <AGENCY>, both internal to <AGENCY> (such as Enterprise Architecture standards) and external to <AGENCY> (such as NIST guidelines).
13. The Contractor shall provide a program-level Test and Evaluation Master Plan (TEMP). The TEMP shall define the methods, scenarios, personnel, facilities, and other resources that will be used for testing.
14. The Contractor shall provide SAT Test Plans as needed for Task Orders (SE Projects) under <AGENCY> projects. The SAT Test Plans shall define in detail the methods, scenarios, personnel, facilities, and other resources that independent testers and evaluators will use for testing and updating Test Plans as required.
15. The Contractor shall provide Monitoring Reports following DR testing, and Test and Evaluation reports for SAT, as needed to address detected issues in a timely manner.
16. Test and Evaluation reports shall document findings in sufficient detail to enable corrective actions to be taken by <AGENCY>. Test and Evaluation reports shall reference relevant documents (e.g. Test Plans, DR packages).

## Records Management Services

The Commission is responsible for developing and implementing a records management program that complies with legal, statutory, and regulatory requirements to ensure that adequate and proper documentation is maintained throughout the record life-cycle

The requirements for this service area are:

1. The Contractor shall maintain complete operation and maintenance of a Public Reference Room (PRR) facility in accordance with the Public Reference Room Standard Operating Procedures document in the EAL.
2. The PRR provides fee-for-public information services to the general public, which includes photocopying, printing, and general research of the Commission’s public information and records. The Contractor shall also maintain selected documents for public viewing.
3. The Contractor shall maintain a Records Maintenance Center (RMC) and provide records maintenance services which includes processing records and filings for temporary storage, record inventorying and indexing services, transfer to off-site storage or permanent records to the National Archives and Records Administration (NARA), record retrieval services, and disposition activities. These services shall be provided in accordance with Standard Operating Procedures, <AGENCY> requirements/policies, NARA regulations, and individual task direction by the Program Manager.
4. The Contractor shall maintain and update the Records Management Program (RMP) defined in the Records Management Directive and in accordance with Records Management <AGENCY> Comprehensive Disposition Schedule documents in the EAL. This RMP provides the foundation for records management policy and procedures, records identification and classification, records retention and disposal, and training to a variety of audiences, which complies with Federal and statutory requirements
5. The Contractor shall take a proactive approach to aid in meeting compliance challenges, both existing, new, and emerging, including but not limited to, social media and cloud computing, e-mail management, and NARA directives. These approaches may be in the form of independent assessments designed to ensure that programs are properly documented and in compliance with NARA requirements.

# Task 6 - Systems Engineering (SE) Services

Systems Engineering (SE) supports the <AGENCY> mission by interpreting the strategy and objectives of the Commission and ensuring that technical solutions are in place to support the <AGENCY>. As <AGENCY> establishes new methods of regulating energy, Systems Engineering works closely with each <AGENCY> program office to ensure that their technical requirements are met.

Currently, most of <AGENCY> applications and infrastructure reside on premises at the HQ and the Alternate Computing Facility (ACF). <AGENCY> is in the early execution phases of a long-term program to lessen reliance on internal application and system hosting in favor of cloud services. <AGENCY> is using email on the cloud today. <AGENCY> is conducting market research of additional cloud service providers to see what FISMA compliant offerings are available to support the federal sector. <AGENCY> expects the Contractor to assist with future transitions to the Cloud.

The SE support requirements fall into two general areas: 1) Core Engineering is an ongoing effort associated with streamlining and modernizing the <AGENCY> computing infrastructure, and 2) SE Project Support which is associated with identifying requirements for projects (please see requirements for SE Project Support) and assisting with execution of SE Projects.

## Core Engineering Support

Modernizing information technology and organizational business processes involves integrating hardware and software components and replacing end- of-life technology, all the while maintaining the Commission’s business operations with minimal disruption. <AGENCY>’s IT services include services such as: IT infrastructure (data centers, networks, desktop computers, and mobile devices); enterprise IT systems (Email, collaboration tools, identity and access management, security, and web infrastructure); and business systems (eLibrary, eFiling, eRegistration, eService, ATMS, etc.). To support the IT modernization requirements, the Contractor shall:

* Provide the systems engineering solutions necessary to ensure that <AGENCY>’s systems deliver an increasingly higher level of effectiveness, reliability and performance (technically, functionally and in terms of customer support) while reducing ownership costs. The planning for efficient and reliable systems to reduce ownership costs while improving system performance, combined with strong and up-to-date knowledge of technology solutions are key components of this service. The Contractor shall bring the tools, experience, approaches, and leadership to <AGENCY> to move its information technology environment into a proactive, highly customer responsive system following industry best practices.
* Work with PMO to provide technical systems review, technology assessments, and develop recommendations for streamlining <AGENCY>’s computing and communication systems.
* Review capacity, availability requirements, and ensure that systems are scaled to meet these requirements.
* Review, analyze, and provide <AGENCY> with a roadmap on how best to upgrade and/or replace outdated business systems, infrastructure components, and assess the impact of an upgrade. Support shall include feasibility studies, possible solutions in the marketplace, cost-benefit analyses, impacts on associated or dependent applications, associate interface with other system, transition plans, proposed resources, and operational impacts for both near and long term. <AGENCY> preference is to move these systems to the cloud using application development platforms such as Salesforce.com.

The Core Engineering efforts cover all aspects of <AGENCY> operations, including its hosted applications, internal business systems, and the networking and hosting infrastructures.

## SE Project Support

The Contractor shall assist the CIO with developing the high-level documentation required for analysis and approval decisions of SE Projects. <AGENCY> requires that all SE Project utilize EVM methodology to accurately determine progress and value. In addition, since all of these SE Projects will be performed outside of the operational support efforts, the Contractor’s SE staff shall:

* Work with the PMO and the Project stakeholders in interpreting requirements.
* Assist their development and engineering personnel with interpreting <AGENCY>-specific information.
* Provide working-level knowledge about <AGENCY> systems and their configuration.
* Develop and maintain EVM metrics for all projects as applicable to the effort.
* Assist with creation and execution of test plans.

See Section 12 – SE Project Services for additional project related requirements.

# Contractor's Facility Requirements

## General Requirements

<AGENCY> requires the Contractor to provide a turn-key solution and will not participate in any costs associated with standing up, maintaining or expanding any Contractor’s proposed facility(ies). The Contractor shall assume all responsibility for standing up and maintaining the Contractor’s facility which will meet service demand and performance levels required by <AGENCY>. Contractor-provided facility must be located in the lower 48 contiguous United States (CONUS). Although <AGENCY> does not anticipate significant increase in the level of effort, the Contractor’s facility should be able to handle increased staff levels, which may be needed to fulfill special project requirements on temporary basis.

Specifically, the Contractor shall:

* Provide all computer equipment, printers, plotters, LAN infrastructure, and phone systems for all personnel, except for personnel whose primary duty location is at <AGENCY>
* Perform routine operation and maintenance of all computing devices and systems deployed at the contractor facility that support the <AGENCY> ITS program including, but not limited to servers, workstations, monitors, printers, other peripherals, and network infrastructure components (routers, hubs, switches, circuits, etc.), which are provided by the Government or the Contractor.
* Provide expendable office supplies, such as pens, pads, printers, printer cartridge, etc.
* Be responsible for provisioning and maintaining internal network accounts and permissions.
* Establish and maintain connectivity to the <AGENCY> resources.
* Maintain all equipment, network components, and software to the latest <AGENCY>-approved configuration.

The Contractor’s facility shall provide a backup power system to maintain operations of critical systems during power outages. This can be achieved through a combination of uninterruptible power supplies (UPS) and independent generator power supply. Backup power must be able to be supplied continuously for 14 days. This may be achieved by refueling the generator so long as operation continues while refueling and more than one fuel supplier arrangement exists.

## Information Systems Security Requirements

The Contractor shall assume all responsibility for meeting applicable <AGENCY> security controls and standards. Particularly, the Contractor shall:

* Maintain current anti-virus definition files on all equipment.
* Deploy emergency patches and other upgrades to all equipment as required by the Government policies and regulations.
* Develop and maintain information security materials and briefings to all staff who have access to <AGENCY> upon their assignment to the Task Order, provide updates and refresher training annually, and document staff participation.
* Provide security for all physical facilities and assets used in conduct of the Task Order and develop supporting documentation that complies with all Government regulations and guidance.
* Monitor vulnerabilities and apply security patches per the Vulnerability Management Program (VMP).
* Notify <AGENCY> CO and CIO leadership in the event that a computer virus or virus-like activity is detected at the Contractor’s facility.
* Notify <AGENCY> CO and CIO leadership in the event of an attempted or successful electronic or physical intrusion at the Contractor’s facility.

## Development Lab

The Contractor shall establish a development, integration, test and validation environment that emulates the production environment. The Contractor shall use this Lab to develop and test all new software/systems or enhancements to the current operational systems. The Contractor shall ensure that the lab’s testing elements (and applicable development elements) correctly emulate the current <AGENCY> production environment in a manner which supports immediate release to production.

## Phone System/ACD/IVR Requirements

The Contractor shall provide a phone system capable of supporting and reporting the Service Desk’s operations. The Contractor shall provide an Automatic Call Distribution (ACD) solution that has the following minimum functionality:

* The ACD solution shall execute specific call routing rules or treatment based on incoming toll-free number/Dialed Number Identification Service (DNIS), selected menu option, time of day, day of week, day of months, etc.
* Calls shall be greeted with <AGENCY>-dictated announcement and prompting.
* The ACD solution shall support skill-based call routing to accommodate routing of internal IT support and external customer calls.
* The ACD solution shall support priority queuing (based on call type, Automatic Number Identification (ANI), DNIS, info-digit input, caller wait time, and trunk group).
* The ACD solution shall support programmable routing (and call treatments) based threshold conditions and maximum number of callers in queue.
* Calls shall be provided with specific announcements if number of calls in queue exceeds a configurable maximum number. These calls will be presented with an announcement informing callers of extremely busy conditions and request callers to call back at a later time or to be routed to a voice mail.
* The system shall present callers in queue with both Music-on-Hold and <AGENCY>-specified announcements.
* The solution shall inform callers about an estimated wait time.
* Contractor must provide voice mail for the Service Desk.
* The Contractor’s phone system shall allow authorized off-site personnel to listen in to live conversations.

## Call Reporting Requirements

The Contractor shall provide a Web-based Service Desk call reporting system capable of presenting real time and historical data about call, email, and Web activities. This Contractor provided repository shall be capable of transmitting the above information to a standard based external database using SQL, Java Database Connectivity (JDBC), and/or Open Database Connectivity (ODBC) interfaces.

The reporting tool shall have the flexibility to collect data and distribute reports via “push” or “pull” method, or a combination thereof.

The Call/Contact Type reports shall at a minimum include the following types of data for each type of contact method:

* Number of calls/contacts currently in queue
* Service levels
* Number of calls/contacts offered, handled, queued, and abandoned
* Number of hang-ups/short calls before the ACD queue (i.e., wrong number)
* For historical call reporting (on per hour, per 30 minute, and Busy Hour basis)
* Average and Longest Speed to Answer
* Average Talk Time
* Average Wrap Up Time
* Average Hold Time
* Abandon Rate
* Number of Abandon Calls
* Number of Short Calls
* Longest Wait Time
* Longest Talk Time
* Number of received and associated response times for email requests
* Number of received and associated response times for Web requests
* Number of received and associated response times for fax requests

### Blended Call Handling Requirements

To provide better customer experience regardless of the access method used, <AGENCY> envisions a need to introduce blended call center functionality into the Service Desk. This functionality will not be required at the beginning of the contract; however, <AGENCY> would like to explore the use of a blended call center technology as a means of integrating handling and reporting on multiple means of accessing the SD.

<AGENCY> requires the Contractors to address their capabilities in meeting the requirements listed in bullets below. The Contractor shall provide:

* All hardware and software to enable blended agents, i.e. the routing of incoming contacts from various media (e.g., voice, web chat, email, and text) to the next available agent with the appropriate skills to handle contacts across multiple media.
* A blended agent solution that provides performance statistics across all contact types.
* A blended agent solution that provides a single interface to configure and manage contact routing across all blended media and blended agents.
* A solution that consolidates metrics associated with all contact activity, across all contact channels from contact initiation to termination; i.e., the solution shall have the ability to collect and accurately report on all applicable information from carriers and the network, through to final handling by the Contractor.

## COOP Requirements

The Contractor shall be required to maintain a Continuity of Operations (COOP) solution, which can provide an alternate facility in case the Contractor’s primary facility and/or infrastructure becomes fully or partially unusable due to, among other things, physical building damage, inability of staff to perform their functions, or for any other reasons. The Contractor shall present their approach and capabilities to maintaining continuity of operations as well as time required to establish full functionality in case of full or partial loss of the primary facility(ies).

# Systems Engineering Project Services

## Systems Engineering Project Requirements

<AGENCY> may task the Contractor to perform additional IT-related initiatives, performance of which cannot be accommodated within the constraints of the agreed-upon day-to-day operational support defined in the rest of the Performance Work Statement (PWS). Projects can be proposed by the Government or by the Contractor. Regardless of source, initiation of any work requires a documented proposal and the <AGENCY> CO’s documented approval.

SE Projects shall be under the overall scope of the ITS task order and are limited in duration and scope and shall be managed as separately definable and self-contained work efforts, with a pre-approved time line, requirements, budget, and success criteria.

Projects can be firm-fixed priced or time and material/labor hour and shall be managed according to contract type agreed upon in actual execution.

## Project Concept

The process for initiating an SE Project starts with creation of a Project Concept Plan. Each Project Concept Plan shall contain, at minimum a high- level business case and objectives, approach to meet these objectives including a high-level plan, milestones, and a Rough Order of Magnitude (ROM) cost estimate.

Costs of creating and updating these concept plans shall not be billed separately as these efforts fall within the scope of work defined in the PMO tasking area.

## Project Execution

If <AGENCY> accepts the Project Concept Plan, the project moves into the <AGENCY>’s standard Capital Planning and Investment Control (CPIC) review and decision process.

Consistent with the CPIC Process Control Phase, <AGENCY> will require regular project progress updates or reports with data showing execution against milestones and budget to show status in relation to work completion targets, schedule, and budget constraints, and execution of approved projects shall be integrated into the Contractor’s Task Order Management /project management framework accordingly.

## Product Execution, Delivery and Support

For all projects resulting in a hardware or software product, <AGENCY> requires and Contractor shall ensure that all products adhere to the core requirements listed below:

* Must be bug and defect-free, fully tested, and directly integrate-able with related <AGENCY> systems.
* Must meet all applicable security and policy regulations.

Scope includes support of:

* Transition to the operational environment.
* Ongoing maintenance and bug fix support for a period defined in the individual tasks.
* Must include business continuity.

Specific functions, technical, and performance requirements will be negotiated as part of the project acceptance process.