TASK ORDER

GSQ0014AJ0142

Former Task Order Number: GST0012AJ0003

Open Systems Hosting Services

in Support of:

General Services Administration
Federal Acquisition Service
Office of the Chief Information Officer

ISSUED TO:

CSC Government Solutions, LLC

The Contractor's basic Alliant GWAC contract is applicable to this Task Order

ISSUED BY:

General Services Administration
Federal Systems Integration and Management Center (FEDSIM)
2.100 Crystal Drive (QFOB)
Suite 800
Arlington, VA 20406

FEDSIM Project Number 14066GSM

NOTE: The section numbers in this Task Order correspond to the section numbers in the Alliant Contract. Section C of the contractor's Alliant Contract is applicable to this Task Order and is hereby incorporated by reference. In addition, the following applies:

C.1 PURPOSE

The General Services Administration (GSA), Federal Acquisition Service (FAS), Office of the Chief Information Officer (OCIO) requires information technology (IT) services to manage, support and administer its infrastructure. Infrastructure support services include those activities required to provide Data Center services, Networking and Storage capabilities, and a management framework referred to at Cross Functional IT Services.

FAS' goal is to modernize its IT infrastructure by transitioning to a technical framework that enables rapid response to emerging internet and technology trends and complex Government requirements. FAS also seeks to adapt its legacy applications to more cost-effective technologies e.g., cloud computing, Infrastructure as a Service (IaaS), and virtualization.

C.1.2 BACKGROUND

The FAS OCIO develops and manages applications and systems in support of FAS business lines and staff offices in accordance with policy established by the GSA Chief Information Officer.

GSA FAS currently hosts its open systems infrastructure in two contractor operated data centers and one FAS leased office facility. The specific characteristics of each facility reflect both FAS systems requirements and historical development. In all cases, FAS owns all server, peripheral, and network hardware and software installed in each site, and provides these as Government Furnished Property (GFP) to contractor personnel who conduct day-to-day operations, systems administration, and provide technical support to FAS and FAS stakeholders.

C.1.3 AGENCY MISSION

GSA's FAS assists Federal agencies throughout the world to acquire supplies, furniture, computers, tools, and equipment. The products and services offered to these Federal agencies include office equipment and supplies, laboratory equipment, paint, tools, hardware and software, copiers, furniture, vehicles, and an array of service contracts that support other critical requirements e.g., charge cards and financial management services. FAS Fleet provides vehicle services to Federal agencies, offering a modern fleet and timely replacement of vehicles, lower lease costs, professional maintenance management, and a selection of alternative-fuel vehicles. FAS also helps federal agencies dispose of items they no longer need by transferring them to other government agencies or nonprofit organizations or by selling them to the public.

GSA FAS provides best-value services, products, and solutions to customers that increase overall Government effectiveness and efficiency.

GSA FAS is organized into four primary business portfolios, six supporting integrator offices and 11 Regions.

C.1.4 CURRENT IT/NETWORK ENVIRONMENT

GSA FAS currently has a contract with a single hosting and infrastructure provider that provides hosting services, to include operations and maintenance, administration, network, and related infrastructure service. GSA FAS owns and operates approximately 356 physical servers (identified below) that are located in multiple locations and hosting approximately 50 applications with 15 major applications. FAS is in the process of consolidating hardware components, so the number of physical servers will decrease over time.

The following is a listing of IT assets by location, type, and where they are hosted.

Asset Count	Location	Server or Other Component	Hosted at Government Data Center	Hosted at Contractor Owned Data Center
24	Arlington Computing Center (Dev/Test)	Linux	√	
37	Arlington Computing Center (Dev/Test)	Solaris 9	√	
2	Arlington Computing Center (Dev/Test)	Solaris 10	√	
81	Arlington Computing Center (Dev/Test)	Windows	√	
6	Arlington Computing Center (Dev/Test)	SAN Components	√	
11	Arlington Computing Center (Dev/Test)	Network Components	√	
2	Arlington Computing Center (Dev/Test)	Backup Components	√	
7	Crystal City Lab	Various IT Components 15 VMware instances.	√	
20	Sterling Production	Windows Servers		√
21	Sterling Production	Solaris 9		√
2	Sterling Production	Solaris 10 – M8000 containers		√
20	Sterling Production	Linux		√
19	Sterling Production	Network Components		√
3	Sterling Production	Backup Components		√
8	Sterling Production	SAN Components		√
8	Chicago Production	Linux		√
16	Chicago Production	Solaris 9		√
1	Chicago Production	Solaris 10 – M8000 containers		
7	Chicago Production	Windows		√
8	Chicago Production	SAN Components		√
10	Chicago Production	Network Components		√
3	Chicago Production	Backup Components		√
10	Regional Servers	Windows	√	

C.2 SCOPE

The goal of the FAS OCIO IT hosting environment requirement is to provide timely and cost efficient support services to stakeholders while testing and deploying 'new' system enhancements for the FAS business lines and support offices. GSA FAS OCIO requires Open Systems Hosting and infrastructure services at FAS locations (Government sites) and at the contractor's hosting facility.

GSA FAS will provide all server, peripheral, and network hardware and software needed for open systems and infrastructure services to the contractor as Government Furnished Property (GFP) for provision of the initial services. GFP is provided in Section J, Attachment J of the TOR. During the period of performance of this task order, it is the Government's desire to migrate critical infrastructure services to technologies that enhance efficiency, are robust, and reliable to serve FAS stakeholders. IaaS and "cloud computing" initiatives are two examples that may provide a framework that is more cost-effective and can be adapted to meet the dynamic infrastructure and hosting requirements of the GSA FAS organization and stakeholders. The contractor, as an optional task, shall investigate emerging technologies, industry best practices, and Government regulations and guidelines, and provide recommended solutions and high level migration schedules for the FAS OCIO to consider. Once the Government decides on the best solution, the contractor shall begin to adapt, or migrate the GSA FAS infrastructure environment to IaaS or other hosting paradigm that takes advantage of emerging technologies and moves GSA FAS towards a technology solution that offers more efficient capacity utilization.

The contractor shall support the infrastructure support requirements of the FAS Business Lines and support offices, and the contractor shall provide these services at current levels or better, as determined by the SLAs included in Section J, Attachment H, Award Fee Determination Plan (including those requiring changes), until transition to the selected hosting contractor facilities is complete and accepted by the Government. The contractor's schedule of milestones for hosting transition activities (including all gate reviews and integration testing) shall be provided in the contractor's technical proposal (see Section L). The contractor shall update transition activities if necessary with close oversight and approval by Government personnel.

The contractor shall perform the following activities that are within the scope of the task order, including but not limited to:

- Virtual machine (VM) instances
- Provide support for Solaris 9 and 10, Red Hat Linux, VMware and ~~Windows 2003 and 2008 or higher~~
- Provide support for an EMC and Netapp Storage area network (SAN) which includes SAN switches, LUN provisioning, Network Attached Storage (EMC Celerra), geographic Replication using the RecoverPoint appliance, HBA support and support for PowerPath
- ~~Maintain Network equipment~~
- Maintain Government Furnished Property (GFP) and/or Contractor-owned equipment
- Daily backups
- Support for Sun/Oracle M8000 with Solaris 10 containers
- Support for Sun/Oracle servers running Solaris 9

- System patches
- Anti-virus detection
- Signature updates
- Liaison with GSA FAS Operations manager for infrastructure changes and projects.
- Perform infrastructure changes.
- Gain knowledge of assigned infrastructure components.
- Coordinate and perform changes for the environment.
- Interact with other team members for infrastructure updates

Section C.2.1 provides the current GSA FAS service environment.

C.2.1 GSA FAS SERVICE ENVIRONMENT

GSA FAS currently maintains infrastructure in the following four key locations and selected GSA Regional sites:

1. Sterling, VA (Primary) Data Center (Contractor Owned)

   The Primary data center facility is where production infrastructure is hosted. This location is in full compliance with GSA FAS guidelines for safety, fire protection, un-interruptible power supply (UPS) and security requirements. This facility has two power feeds coming into the center. Safety and security systems include smoke, fire and water protection and detection. Security includes 24-hour guard protection, a complete badge control system, and interior and exterior video surveillance, including motion detection. GFP is currently caged and is isolated from other customers in the same facility.

2. Chicago, IL (Disaster Recovery) Data Center (Contractor Owned)

   The Chicago Disaster Recovery data center is where disaster recovery infrastructure is hosted. This location includes a 7x24 on-site building security, operations, and engineering staff for support of the data center environment. The facility includes fire control and early smoke detection, which is monitored by the Building Maintenance System that provides audible alarms and radio dispatch of facility support personnel. GFP is currently caged and is isolated from other customers in the same facility.

3. Chantilly, VA (Development and Test) Computing Facility (Government Owned)

   The Development and Test data center, located in Chantilly, VA, is where development and testing infrastructure is hosted. This location is used by GSA FAS for hosting both development and testing environments for the core applications. The facility includes fire detection and an UPS for conditioning the power feed. The contractor shall assist with the management of the GSA FAS Data Center located in Chantilly, VA. This is a GSA FAS-leased office facility which houses GSA FAS Test and Development IT assets. The Government intends to continue to host these IT assets at the Chantilly Computing Facility, until alternative hosting paradigms are implemented. Contractor management responsibilities include:

   - ~~Coordinating network maintenance with other organizations within GSA;~~

- Cabling maintenance; and
- Assisting with the installation of new hardware

~~The contractor shall provide remote support for Windows servers and future ECMS servers located in GSA Regions.~~

C.3 OBJECTIVE

The objective of the task order is to provide IT services to support the GSA FAS infrastructure through outsourced Open Systems Hosting Services. The contractor shall accomplish the following objectives:

- Assure a "low risk" transition with minimal disruption to business activities and minimum disruption to GSA FAS IT activities.
- Continue to provide and improve upon high quality service levels to stakeholders.
- Continue to provide and improve upon IT systems quality, availability, security, and integration.
- Assist GSA FAS evaluate, test, and adapt legacy applications through the use of cost-effective technologies like virtualization, cloud computing, and IaaS. GSA FAS seeks to move smaller, moderate, or larger portions of the current server and storage environment to one or a combination of these hosting paradigms.
- Minimize operating costs by leveraging matrix resources (non-dedicated resources) and in the future migrate to more cost-effective technology platforms.
- Institute an expanded, more systematic use of Service Level Requirements (SLRs) and enforceable performance measurement (See Section J).
- Investigate emerging technologies, and recommend services that can leverage operational scale and best practices to achieve optimal cost and service level performance.
- Adopt a flexible and variable cost structure to accommodate unforeseen business requirements, surges in capacity, etc.
- Utilize the contractor’s automated tools to implement administration processes, establish a Configuration Management Database (CMDB) that includes configuration interactions between operating systems, network components, databases and applications required to support FAS servers and network components.
- GSA FAS intends to leverage the contractor’s tools, which shall be provided as a service, to manage, monitor and maintain the FAS infrastructure. These tools shall also be leveraged as a method to implement the management framework that GSA FAS is requiring.
- Optimize equipment monitoring through the use of dashboards that collect and report system alerts real-time for all critical IT assets (production at a minimum).Utilize ongoing feedback mechanisms in the form of a bi-annual review to ensure that performance meets GSA FAS stakeholder expectations.

C.4 TASKS

The contractor shall perform the following tasks to meet the objectives of the task order.

C.4.1 TASK 1 – PROVIDE PROJECT MANAGEMENT

The contractor shall provide project management support under this task order. This includes the management and oversight of all activities performed by contractor personnel, including subcontractors (if applicable), to satisfy the requirements identified in this Performance-Based Statement of Work (PBSOW). The contractor shall identify a Project Manager (PM) by name, who shall provide management, direction, administration, quality assurance, and leadership of the execution of this task order.

C.4.1.1 SUBTASK 1 – COORDINATE A PROJECT KICK-OFF MEETING

The contractor shall schedule and coordinate a Project Kick-Off Meeting at the location approved by the Government (in Crystal City, Arlington, VA) no later than 15 calendar days after task order award. The meeting shall provide an introduction between the contractor personnel and Government personnel who will be involved with the task order. The meeting will provide the opportunity to discuss technical, management, and security issues, and travel authorization and reporting procedures. At a minimum, the attendees shall include vital contractor personnel, representatives from the FAS OCIO, other FAS offices, other Government stakeholders, the FEDSIM Contracting Officer's Representative (COR) and the FAS OCIO Technical Point-of-Contact (TPOC). The contractor shall provide the following at the Project Kick-Off meeting:

- Transition-In Plan Overview Briefing
- Project Management Plan (including service performance metrics)
- Earned Value Management (EVM) Plan

C.4.1.2 SUBTASK 2 – PREPARE A MONTHLY STATUS REPORT (MSR)

The contractor's Project Manager shall develop and provide a MSR (see Section J, Attachment A) using MS Office Suite applications, by the 15th of each month via electronic mail to the COR and TPOC. The MSR shall include 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 issues or concerns and proposed resolutions to address them
- Personnel gains, losses and status (MBI status, etc.)
- Government actions required

- Schedule (Shows major tasks, milestones, and deliverables; planned and actual start and completion dates for each)
- Summary of trips taken, conferences attended, etc. (Attach trip reports to the MSR for reporting period)
- EVM statistics and FAS Open Systems Availability
- Accumulated invoiced cost for each CLIN up to the previous month
- Projected cost of each CLIN for the current month
- Comparison data / monthly performance reports

C.4.1.3 SUBTASK 3 - EARNED VALUE MANAGEMENT (EVM) CRITERIA

The contractor shall employ and report on EVM in the management of efforts executed under the CPAF identified tasks within this task order. See Section H.19, Earned Value Management**,** for the EVM requirements.

The contractor shall employ and report on EVM in the management of project efforts executed under the CPAF identified tasks within this task order which exceed $250,000 in value or have been designated as high priority projects by the COR. See Section H.19, Earned Value Management**,** for the EVM requirements.

C.4.1.4 SUBTASK 4 – CONVENE TECHNICAL STATUS MEETINGS

The contractor Program Manager shall convene a monthly **Task Order Activity and Status Meeting** with the COR, TPOC, and other Government stakeholders. The purpose of this meeting is to ensure all stakeholders are informed of the monthly activity and status report, provide opportunities to identify other activities and establish priorities, and coordinate resolution of identified problems or opportunities. The contractor's Program Manager shall provide **Technical Status Meeting Minutes**, including attendance, issues discussed, decisions made, and action items assigned, to the COR within fifteen (15) days following the status meeting.

C.4.1.5 SUBTASK 5 – PREPARE A PROGRAM MANAGEMENT PLAN (PMP)

The contractor shall document all TO support requirements in a **PMP**. The PMP shall detail Standard Operating Procedures (SOPs) for all tasks. The 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 milestones, tasks, and subtasks required in the TO. The PMP shall provide for a Work Breakdown Structure (WBS), and associated responsibilities and partnerships between Government organizations by which the contractor shall manage all work. The PMP shall include the contractor's Quality Management Plan (QMP) and EVM Plan.

The contractor shall perform according to the Service Level Requirements identified in the QASP (see Section J) and the contractor's Government-approved QMP. The contractor shall document any changes to these documents in the PMP.

The contractor shall provide the Government with an initial Draft PMP at the Project Kick-Off Meeting, on which the Government will make comment. The contractor shall incorporate Government comments and provide a revised PMP to the Government no later than two (2) weeks after receipt of Government comments. The delivery schedule for the PMP and other TO deliverables is provided in Section F of the TOR.

C.4.1.5.1 UPDATE THE PROJECT MANAGEMENT PLAN (PMP)

The PMP is an evolutionary document that shall be updated yearly. The contractor shall work from the latest Government approved version of the PMP.

C.4.1.6 SUBTASK 6 – PREPARE TRIP REPORTS

The Government will identify the need for a Trip Report (if required) when the request for travel is submitted. The contractor shall keep a summary of all long-distance travel, to include, at a minimum, the name of the employee, location of travel, purpose of trip, trip duration, and POC at the travel location.

C.4.1.7 SUBTASK 7 – PROVIDE CUSTOMER FEEDBACK SURVEYS

The contractor shall establish and implement a methodology for providing customer feedback. This shall include processes, procedures, and capabilities to assess: customer satisfaction, emerging requirements, and developing trends. The contractor shall also implement processes / procedures and communication media to keep stakeholders and functional proponents informed of the project's status, future plans, and opportunities.

C.4.2 TASK 2 – PROVIDE TRANSITION MANAGEMENT SERVICES

The contractor shall implement a transition in methodology contained in their Government-approved Transition-In Plan (see Section C.4.2.1) that is based on the contractor's transition approach presented in their technical proposal to ensure that contractor personnel and subcontractor personnel (if applicable) provide a seamless, risk mitigated, and effective transition. The contractor shall ensure that transition activities do not disrupt FAS services to stakeholders. Transition management services include FAS servers and FAS-provided GFP network cables, switches, firewalls, and routers from the current FAS contractor operated service / data centers to the contractor's proposed IT hosting facilities. Contractor transition responsibilities shall include transition planning, packing, moving, installation, and testing of FAS servers and FAS-provided GFP network cables, switches, firewalls, and routers.

All Transition activities shall be completed no later than 120 days after Government approval of the Transition-In Plan.

Within the 120 day transition-in period, the Government will provide the contractor with necessary Government Furnished Information (GFI) and GFP. During the transition period, the existing contractor providing hosting support shall remain responsible for all system sustainment

activities until officially relieved by the Government and the new contractor assumes full responsibility.

The transition shall ensure minimum disruption to vital Government business. The contractor shall ensure that there will be no service degradation during and after transition. The contractor-developed, detailed Transition-In Plan shall provide for, at a minimum, the following:

- An overview of the transition effort
- An updated (if needed) schedule with milestones and tasks
- Description of systems and GFP to transition
- Transition of GFP/Government Furnished Information (GFI)
- Transition knowledge and information from key contractor personnel
- Transition knowledge and information regarding risk or problem areas

The contractor shall provide a Transition-In Plan Overview Briefing at the Project Kick-Off meeting. See Sections H.27 and H.28 for additional information about Transition In and Transition Out activities.

C.4.2.1 SUBTASK 1 – TRANSITION-IN PLAN

The Contractor shall deliver a **Transition-In Plan** to include a plan for the transportation of GFP and transition notices that is based on the contractor's transition strategy as presented in their technical approach. The Transition-In Plan shall incorporate a phased approach enabling GSA FAS to maintain continuity of infrastructure and hosting services throughout the transition. The transition shall include moving equipment from the current location to the new location and establishing network connections to the GSA FAS infrastructure to ensure no downtime of services. Equipment is to be caged and not co-located.

- The Contractor shall deliver a Transition-In Plan that addresses the following requirements at a minimum: The Transition-In Plan shall identify all project management, procedures and tools to be used to manage the transition;
- The Transition-In Plan shall detail the impacts of transition, equipment ownership, GFP/space, and a complete detailed schedule for transition, focusing on ensuring business continuity throughout transition;
- The Transition-In Plan shall also define contractor's approach to staffing, progress reporting, coordination with third-party providers, and customer education and communication

The contractor shall provide a draft Transition-In Plan within 45 days after task order award. The final Transition-In Plan shall be delivered to the Government no later than 90 days after task order award. The contractor shall coordinate its proposed sequence for transitioning sites with GSA FAS and shall make adjustments to the sequence, in coordination with GSA FAS OCIO prior to making the Transition-In Plan final. The contractor shall submit the final Transition-In Plan to the GSA FAS Information Systems Security Officer (ISSO) for approval. The contractor

shall not proceed with transition without obtaining GSA FAS OCIO and ISSO approval of the Transition-In Plan in its entirety or in part.

The contractor shall provide integration and testing activities as part of the transition. The contractor shall provide integration and testing activities associated with ensuring that all individual GSA FAS data center components have been properly moved, installed, configured and deployed to provide a fully functioning data center service to GSA FAS internal customers and to achieve a seamless transition. The contractor shall develop and document an Integration and Testing Plan as part of the Transition-In Plan. The contractor shall manage the integration test environment and conduct integration and security testing for all moved, new and upgraded equipment, networks based on requirements defined in GSA FAS and Federal security documents that will be provided at the Project Kick-Off Meeting.

For all new equipment, the contractor shall evaluate all new and upgraded system components and services for compliance with GSA FAS security rules, regulations and procedures. The contractor shall assess and communicate the overall impact and potential risk to system components prior to implementing changes. The contractor shall develop, conduct and document User Acceptance Tests (UAT) requirements.

C.4.2.1.1 TRANSITION TRANSPORTATION SECURITY

The contractor shall incorporate the following GSA FAS-specific transportation security requirements, at a minimum:

- GSA FAS must review and approve the qualifications of any personnel (including sub-contractors) involved in the physical moving of equipment
- Only personnel approved by GSA FAS shall have physical or logical access to equipment during the move
- All equipment must be transported safely, securely, and with minimal risk of damage and loss of data
    - All GSA FAS assets shall be inventoried, tagged, and verified by GSA FAS personnel before and after the move
    - GSA FAS personnel will inspect the inventory before a seal is put on, and remove the seal at the destination

C.4.2.2 SUBTASK 2 - PROVIDE TRANSITION OUT SUPPORT

The contractor shall support the Government during transitioning out of the task order. The contractor shall prepare a Transition-Out Plan that details all transition out activities, to include both contractor and Government personnel roles, to ensure that there is a seamless transition to an incoming contractor /Government personnel at the expiration of the task order. The contractor shall provide a Transition-Out Plan no later than (NLT) 30 days prior to expiration of the TO. The contractor's Transition-Out Plan shall identify how the contractor shall coordinate with the incoming contractor and Government personnel to transfer knowledge regarding the following:

- Project management processes
- Points of contact
- Location of technical and project management documentation
- Status of ongoing technical initiatives
- Appropriate contractor to contractor coordination to ensure a seamless transition.
- Transition of Key Personnel roles and responsibilities
- Transfer of any GFI/GFP
- Identify schedules and milestones
- Identify actions required of the Government

The contractor shall establish and maintain effective communication with the incoming contractor/Government personnel during the transition out period via weekly status meetings or other Government-approved transition communication methodology.

C.4.3 TASK 3 – PROVIDE OPEN SYSTEMS HOSTING SERVICES

The contractor shall provide open systems infrastructure services to include data center hosting services for GSA FAS OCIO. The contractor shall manage and perform Open System services transparently and without regard to technology platform, using the *Information Technology Infrastructure Library (ITIL) version 3.0* framework or other proven methodologies for service management. The contractor is also encouraged to propose continuous improvement approaches based on the *Lean Six Sigma* or similar methodology. Section J, Attachment L provides additional detail about the GSA FAS Network environment.

C.4.3.1 SUBTASK 1 – PROVIDE GENERAL DATA CENTER SERVICES

The contractor shall comply with GSA FAS policies, standards, and regulations applicable to GSA FAS including information systems, personnel, physical and technical security. The contractor shall manage event and workload processes across all platforms. The contractor shall provide access to their hosting facility to third party technical support personnel, as needed, for all hardware/equipment of the Data Center.

The contractor shall provide and support Data Center (e.g., ~~LAN~~, WAN connection) and related operations (e.g., procure, design, build, systems monitoring, Incident diagnostics, troubleshooting, Resolution and escalation, security management, and capacity planning/analysis) to meet GSA FAS infrastructure and hosting requirements.
The contractor shall implement and coordinate all GSA FAS-approved changes to the Data Center including those that may affect the service levels of any Hosting Services Third Parties. For Contractor-owned equipment and GFP, the contractor shall provide storage management services.

The contractor shall host and provide facilities support for GSA FAS Production hardware components and IT assets. All GFP in Government facilities will remain as such.

C.4.3.1.1 GENERAL NETWORK SERVICES

GSA FAS shall leverage the Contractor's network backbone for all network services including internet and VPN connectivity. The Contractor's technical approach shall address their network capabilities. GSA FAS OCIO will provide as GFP all servers, firewalls, and routers needed to establish and maintain network connectivity. GSA FAS, in coordination with the GSA Chief Information Officer (CIO), will be responsible for providing, configuring and maintaining two Cisco 7500 series routers that are used to terminate VPN tunnels at the GSA network backbone.

The contractor shall provide the following network services:

- Multiple data center facilities with Tier 1 and Tier 2 networking capabilities (for both the primary and disaster recovery data centers). Data center facilities shall be optimized for security and provision of high quality computing services
- Capability to host servers, firewalls, and routers with a mix of throughput rates of 100 Mbps and 1 Gbps
- Capability to provide, at a minimum, throughput rate of 100 Mbps
- Capability to provide fully redundant local access to high speed WAN capabilities
- Hosting services capable of supporting network connectivity to GSA Corporate Information Network (CIN). The contractor shall provide the capability to establish and maintain network connectivity to support authorized user access
- Hosting Services capable of supporting internet connectivity
- Recommend WAN / VPN
- For contractor-owned equipment, procure/provision and maintain all network components and circuits

C.4.3.1.2 NETWORK OPERATIONS AND ADMINISTRATION

The contractor shall provide network operations activities to include, but not limited to, the following:

- Provide LAN / WAN connectivity contained in the service environment
- Work with public carriers and other circuit providers to perform any operations activities (e.g., provisioning, problem management)

The contractor shall provide network administration services to include, but not limited to, the following:

- Manage Provisioning Internet Protocol (IP) addresses

Section J, Attachment P includes further details regarding the GSA FAS web environment.

C.4.3.3 SUBTASK 3- PROVIDE ENVIRONMENT AND FACILITIES SUPPORT

The contractor shall understand and document all Environment and Facilities Support requirements. The contractor shall review and approve documented Environment and Facilities

Support requirements, and identify requirements for GSA FAS Environment for contractor-supported components. The contractor shall develop, document, and maintain Environment and Facilities Support procedures in a Standards and Procedures Manual. The contractor shall deliver the Standards and Procedures Manual in accordance with the Government-approved PMP. The contractor shall review Environment and Facilities Support procedures. For contractor-owned equipment, the contractor shall coordinate and implement all GSA FAS OCIO approved upgrades and installations with the TPOC or designee. The contractor shall coordinate GSA FAS site activities of all personnel (i.e., contractor employees and others) working in equipment locations (e.g., equipment rooms, Network equipment closets). The contractor shall ensure that facilities support activities conform to the requirements of defined Change Management processes.

The contractor shall meet the requirements as they pertain to the Primary and Disaster Recovery Facilities outlined in Section J, Attachment I.

The contractor shall ensure controlled access to the GSA FAS IT assets within their facilities.

C.4.4 TASK 4 – PROVIDE INFRASTRUCTURE OPERATIONS AND ADMINISTRATION

The contractor shall provide operations and administration services associated with the day-to-day management of the FAS infrastructure environment, which includes the IT assets in the Arlington Computing Center, , the server assets in FAS regions, and all transitioned Production assets. The contractor shall provide and support a stable infrastructure and effectively and efficiently perform operational and processing procedures to ensure the infrastructure meets Service Level Requirement performance targets.

The responsibilities of the contractor include, but are not limited to the following:

- Develop, document and maintain in the Standards and Procedures Manual, Operations and Administration procedures that meet requirements
- Develop operational documentation (i.e., Run Books, Contact Lists, Operations scripts, etc.) that meets GSA FAS requirements
- Identify Enterprise System Management tools to monitor the IT infrastructure and GSA FAS applications
- Deploy enterprise Hosting Services component management tools to monitor the IT infrastructure and, GSA FAS applications as identified
- For GFP and Contractor-owned equipment, install and configure enterprise Hosting Services component management tools in such a fashion that Problems, issues and events are proactively identified, reported and Resolved according to prescribed Service Level Requirements
- Perform event management monitoring of IT Services to detect abnormal conditions or alarms, log abnormal conditions, analyze the condition and take corrective action
- For GFP and Contractor-owned equipment, manage hardware, software, peripherals, services, and spare parts to meet Service Level Requirements, minimize downtime and minimize GSA FAS resource requirements

- Manage and coordinate subcontractors and Third Parties in order to meet Service Level Requirements
- Develop and provide operational reports (daily, weekly, monthly) that provide status of operational activities, production issues and key operational metrics
- Provide GSA FAS with a copy of or access to any Contractor or Third Party-supplied documentation (including updates thereto)

C.4.4.1 SUBTASK 1 – INFRASTRUCTURE SUPPORT

The contractor shall provide the following IT services for the following GSA FAS infrastructure components. See Section J, Attachments J through P for additional information regarding the GSA FAS environment.

C.4.4.1.1 WEB SERVERS

The contractor shall provide the following web server IT support for FAS web servers:

- Provide IT support for ~~iPlanet,~~ Apache, and IIS configurations;
- Provide on-going maintenance, configuration, and optimization of all web servers including application of patches and upgrades;
- Secure web server instances and remediate vulnerabilities;
- Monitor and report status of web servers and related components;
- Provide Apache, Unix ~~the~~ overall architecture and planning support for the web server/DMZ infrastructure;
- Provide expertise with SQUID proxy servers, running on three servers, two in production, and one in Development and Test; and

C.4.4.1.1.1 RESERVED

F5 LOAD BALANCER SETUP FOR GEOGRAPHIC LOAD BALANCING

C.4.4.1.2 DATABASE SERVERS AND OTHER KEY APPLICATION SERVERS

The contractor shall provide the following Oracle/Sun IT support for the primary, and disaster recovery sites:

- Unix, Solaris 9, Solaris 10 and Sun hardware support, especially for the Sun M8000 and M5000
- Creation and management of Sun domains and management of Solaris 10 containers
- On-going maintenance, configuration, and optimization of all Oracle/Sun components
- Provide upgrade support to Oracle/Sun for upgrades, patches, issue resolution and troubleshooting
- Manage the Oracle/Sun M8000 and M5000; provide support for SAN and network integration
- Provide expertise for Solaris 9 and Solaris 10 system configuration and optimization

- Overall architecture and planning support for the Oracle/Sun infrastructure
- Plan and architect technology refreshes and consolidation activities in coordination with GSA FAS OCIO

C.4.4.1.3 DOMAIN NAME SYSTEM (DNS) SERVERS

The contractor shall provide the following IT support for the DNS servers at each site:

- DNS technology
- Support and on-going maintenance, configuration of all DNS servers
- Manage the DNS servers, including DNS record creation and deletion

C.4.4.1.3.1 RESERVED

C.4.4.1.3.2 RESERVED

C.4.4.2 SUBTASK 2 – PROVIDE OPERATIONS SERVICES

The contractor shall provide operations services in support of servers and peripherals located at the contractor's hosting site(s) and operations support services for servers located at GSA FAS facilities (e.g., Arlington, VA, and GSA Regions). The contractor shall provide operations services 24 hours per day, 7 days per week, and 365 days per year except for GSA-approved, prescheduled maintenance down time. The contractor shall provide server monitoring and response to server alerts 24 hours per day, 7 days per week, and 365 days per year.

The contractor shall monitor and operate the mainframe printers at the Government's Washington DC, location at 1800 F St NW to ensure that they are operating properly in accordance with standard operating procedures. The contractor shall assign a full-time printer room operator to perform this service. The Government will provide a workspace for the printer room operator.

C.4.4.3 SUBTASK 3 – PROVIDE SYSTEMS ADMINISTRATION SERVICES

The contractor shall provide systems administration support for GSA FAS Open Systems and Solaris and Linux servers located at contractor-hosted facilities and GSA FAS facilities. The contractor shall provide systems administration support from 6:00 a.m. until 6:00 p.m. Eastern Time, Monday through Friday, excluding Government holidays. The contractor shall provide systems administration support at other times as required to meet surge requirements, technology transfers, and other critical events. The COTR and COR will notify the contractor of these other unique system administration support requirement timeframes to enable the contractor to provide the required resources.

The contractor shall assist GSA FAS application support staff with normal support issues including:

- Application window availability/functionality issues;
- Unix and Linux System connectivity issues;
- Recovery of files, as needed, provided the request is not above the level of security granted for the user

The contractor shall define monitoring requirements and policies, and develop and document in the Standards and Procedures Manual monitoring procedures that meet requirements and adhere to defined policies. The contractor shall provide proactive and scheduled console monitoring of infrastructure and availability of the operating system (e.g., Unix/Linux hardware, network), respond to messages and take corrective action as required. The contractor shall develop and maintain standard automated scripts to perform monitoring on systems operating software. The contractor shall identify and report problems including system, file, disk and application availability problems. The contractor shall provide troubleshooting, repair and escalation of problems in the data center computing environment, as well as provide preventative measures for proactive monitoring and self-healing capabilities to limit outages that impact service delivery. The contractor shall identify and report application availability problems, and assist in resolving application availability problems in accordance with service level requirements and escalate as required. The contractor shall define system administration requirements and policies, and develop and document in the Standards and Procedures Manual procedures for performing system administration that meet requirements and adhere to defined policies. The contractor shall set up and manage application owner accounts, perform access control, manage files and disk space and manage transaction definitions, and, perform system or component configuration changes necessary to support computing services in conformance with change management requirements. The contractor shall provide Usage Statistics Reports that will be used to support chargeback and other reporting requirements.

C.4.4.4 SUBTASK 4 - PROVIDE STORAGE AND DATA MANAGEMENT

The contractor shall provide storage and data management services associated with the provisioning and day-to-day management of the installed Data Center storage and data environment (e.g., direct access storage devices (DASD), redundant array of independent disks (RAID), storage area network (SAN), network-attached storage (NAS), (tape and optical), providing a stable supporting infrastructure and effectively and efficiently performing procedures to ensure services meet Service Level Requirement targets and requirements. Section J, Attachment O provides further details regarding the GSA FAS storage environment.
The contractor shall provide the following SAN support capabilities for all environments:

- Provide knowledge and hands-on expertise in all of the above-mentioned technologies
- Provide on-going maintenance, configuration and optimization of all SAN components
- Provide upgrade support to EMC/Netapp for code upgrades, issue resolution and troubleshooting
- Manage the SAN using EMC/Netapp and other tools
- Monitor and report capabilities of the SAN and related components

- Provide file expansion, RAID group management, LUN provisioning, RecoverPoint configuration, new system additions and data migration
- Configure and maintain PowerPath, Emulex HBA and Cisco MDS SAN switches
- Provide overall architecture and planning support for the SAN infrastructure
- Plan and architect technology refreshes
- Open trouble tickets with EMC

The contractor shall provide off-site back-up media storage for each off-site hosting facility that meets GSA FAS off-site storage requirements for each hosting site proposed by contractor. The back-up media storage shall reside in a location that is at least five (5) miles from the contractor-proposed hosting site that it supports and meets GSA FAS OCIO requirements for back-up and recovery. These locations shall provide physical, environmental, and security capabilities to assure that stored media are well protected and easily accessed. Tapes designated for off-site storage shall be removed from the data center once daily. The contractor staff shall obtain prior approval from GSA FAS OCIO TPOC or designee for schedule changes. The contractor shall arrange pickups, as needed, to ensure that off-site back-up tapes are never retained on site for more than 12 hours. The contractor shall demonstrate their capability to recover media within three (3) hours of notification by GSA FAS OCIO TPOC or designee, or as required by applications processing procedures.

The contractor shall perform the following Storage and Data Management requirements:

- Recommend contractor-standard Storage and Data Management procedures
- Develop, document and maintain in the Standards and Procedures Manual Storage and Data Management Contractor procedures that meet GSA FAS requirements and adhere to GSA FAS policies
- Provide data storage services (e.g., RAID array, SAN, NAS, tape, optical, etc.)
- Monitor and control storage performance according to technical Specifications, Storage and Data Management policies and perform tuning as required
- Perform data and file backups and restores per established procedures and Service Level Requirements
- Maintain and improve storage resource efficiency
- Manage file transfers and other data movement activities
- Provide input processing, for activities such as loading Third Party media (e.g., tape) and receipt and/or transmission of batch files
- Acquire and manage consumables, such as tape, disks, etc., in support of the backup requirements. Coordinate acquisition of additional materials as needed
- Recommend contractor standard Media Operations procedures
- Develop, document, and maintain in the Policies, Standards, and Procedures Manual Media Operations procedures that the contractor shall perform that meet GSA FAS requirements and adhere to GSA FAS policies
- Maintain a media library and media management system
- Manage the media inventory to ensure that adequate media resources are available. Coordinate acquisition of additional media as needed
- Manage input media availability to meet processing Service Level Requirements;

- Load and manage Third Party media
- Provide secure offsite storage for designated media and transport media to GSA FAS approved offsite location as required
- Perform periodic audits to ensure proper cataloging of media

C.4.4.4.1 NETWORK SECURITY SERVICES MANAGEMENT

The contractor shall maintain physical and logical security of assets. The contractor shall conduct periodic security checks per requirements, reporting security violations if found, and assist with resolving said security violations. The contractor shall perform systems security hardening and security vulnerability remediation on GSA FAS systems.

The contractor shall assist GSA FAS Security Operations Center (SOC) which is responsible for performing the following functions:

- Security Event and Information Management Services
- Log Aggregation Services
- Intrusion Detection System Installation, Configuration, Monitoring and Administration;
- Continuous Firewall Installation, Configuration, Monitoring, Administration and Auditing
- Network Forensics Analysis
- Net-flow Anomaly Detection
- File Integrity Monitoring
- Web Application for Firewall Installation, Configuration, Monitoring and Administration and Management
- End User Analytic services
- Security Firewall Management
- Security Intrusion Detection Services
- Security Penetration Services
- Security Incident and Audit Management Services
- Support the SOC and FAS Infosec for certification and accreditations

C.4.4.5 SUBTASK 5 – PROVIDE SECURITY

The contractor shall provide security services associated with maintaining physical and logical security of all Hosting Services components (hardware and software), data, virus protection, access protection, and other Security Services in compliance with GSA FAS Security requirements and all applicable regulatory requirements. The GSA FAS infrastructure at its high water mark is FISMA moderate. All security-related tasks performed by Contractor shall be in conjunction with GSA FAS Security Operations Center (refer to the Network Security Services Management Section).

The contractor shall be responsible for, but is not limited to, the following security requirements:

- Assist in modifying and updating security standards, policies, and procedures
- Participate in and support the weekly Security CAB.

- Review and provide inputs and updates to the Standards and Procedures Manual Security requirements, standards, procedures, and policies including regulatory requirements
- Remain up to date with current Security trends, threats, common exploits, and security policies and procedures and best practices
- Implement physical and logical Security plans in conjunction with GSA FAS Security Operations Center and GSA FAS Security policies and industry standards
- Perform and/or coordinate the approval of log-on/Security-level access changes as detailed in profiles and policies for Hosting Services
- Report Security violations to GSA FAS per GSA FAS policies
- Follow INFOSEC guidance in the resolution of Security violations that originate outside of the hosted Network(s) (e.g.,shut down server, provide logs, etc.)
- Review all nCircle reports and various Security advisories to notify GSA when patches relevant to the IT environment are available and classify the need and speed in which the Security patches should be installed as defined by Security policies
- Maintain ~~all~~ documentation required for Security assessments, audits and internal control and control testing
- Place and support systems with particularly sensitive data in controlled access areas. Only End Users with current, authorized access permission shall be allowed to enter these areas
- Research and investigate vulnerabilities and findings from GSA OCIO managed Infosec scanning tools
- Enforce and support GSA's Security Awareness Program
- Manage and maintain Tripwire on FAS servers and other components

C.4.4.6 SUBTASK 6 – PROVIDE BACK-UP AND RECOVERY

The contractor shall provide back-up and recovery services associated with providing ongoing back-up and recovery capabilities according to GSA FAS schedules and requirements. The contractor shall demonstrate that they will consistently meet or exceed the GSA FAS ongoing back-up and recovery requirements. Currently, GSA FAS uses EMC Networker for the Open Systems environment.

The contractor shall provide the following backup support services at each remote hosting facility:

- All backup capabilities, including management of the backup software, administration and support, and management of the dedicated backup servers
- Monthly full backups, weekly full backups and daily incremental backups of the files and directories as specified by GSA FAS
- Restoration of an individual file or folder upon request as outlined in the Service Level Requirements (SLR)
- Backup on media appropriate for long-term off-site storage
- Backup of virtual machine files
- Administration, maintenance, and testing of all virtual machine and system backups in accordance with GSA standards

- Annual permanent backups will be retained with the first full backup serving as the first annual backup and the anniversary date for permanent backups
- Maintenance of logs of scheduled and ad hoc data backup and restore requests (providing such log reports as requested by GSA FAS). The log report shall, at a minimum, show job date/time, target systems, success/failure status, time to complete and total size of data
- Quarterly test restore to validate backup job success and include details on the test restore in the appropriate monthly status report
- Recommend best practices for Backup and Recovery Services strategies, policies and procedures
- Develop, document and maintain in the Standards and Procedures Manual, Backup and Recovery schedules and procedures that adhere to GSA FAS requirements and policies;
- Manage backup media inventory (tape, disk, optical and other media type), including the ordering and distribution of media
- Perform Hosting Services component backups and associated rotation of media;
- Archive data media at a secure off-site location
- Ensure ongoing capability to recover archived data from media as specified (backward compatibility of newer backup equipment)
- Test backup media to ensure incremental and full recovery of data is possible and ensure Hosting Services component integrity, as required or requested by GSA FAS; and
- Recover files, file system or other data required from backup media, as required or requested by GSA FAS

C.4.4.6.1 IT SERVICE CONTINUITY AND DISASTER RECOVERY

The contractor shall provide IT Service Continuity and Disaster Recovery Services to include the activities associated with providing prioritized IT Service Continuity and Disaster Recovery Services for GSA FAS applications and their associated infrastructure (e.g., CPU, servers, data, and output devices). GSA FAS applications and associated infrastructure services shall receive Disaster Recovery Services according to an analysis of GSA FAS business impact. The contractor shall demonstrate that it will consistently meet or exceed GSA FAS IT Service Continuity and Disaster Recovery Services requirements. Additional information is provided in Section J, Attachment R, "Disaster Recovery System Prioritization." The contractor's responsibilities include, but are not limited to the following:

- Recommend best practices for IT Service Continuity and Disaster Recovery Services strategies, policies and procedures
- Document IT Service Continuity and Disaster Recovery Services procedures that adhere to GSA FAS requirements and policies
- Assist GSA FAS in other IT continuity and emergency management activities (e.g., semi-annual Disaster Recovery drills)
- Develop and maintain a detailed Disaster Recovery Plan to meet IT Service Continuity and Disaster Recovery requirements. The Disaster Recovery Plan shall include plans for data, backups, storage management and contingency operations that provide for recovering GSA FAS systems within established recovery requirement time frames after a disaster affects GSA FAS' use of the Services

- Establish processes to ensure Disaster Recovery plans are kept up to date and reflect Changes in GSA FAS environment
- Perform scheduled Disaster Recovery tests per GSA FAS policies
- Track and report Disaster Recovery test results to GSA FAS
- Develop action plan to address Disaster Recovery testing results
- Implement action plan and provide ongoing status until completion;
- Initiate the Disaster Recovery plan in the event of a contractor Disaster Recovery situation and notify GSA FAS per Disaster Recovery policies and procedures; and
- Support GSA FAS warm standby database servers at the COOP site

C.4.4.7 SUBTASK 7 – PROVIDE ACCOUNT MANAGEMENT

The contractor shall provide Account Management Services associated with the ongoing management of the service environment. The contractor shall develop, document, and maintain in the Standards and Procedures Manual, Account Management procedures that meet requirements and adhere to defined policies. At Task Order award GSA FAS will provide access to Government Wiki.

C.4.4.8 RESERVED

C.4.4.9 SUBTASK 9 – PROVIDE CRYSTAL PARK 4 (CP4) MOVE SUPPORT

The Contractor shall:

- Provide assistance with the discovery/identification phase of all existing HW (Physical and Virtual servers, network switches, SAN, storage devices etc.) in the CP4 data center currently being used to support the FAS Development and Test environments. The Contractor shall review the inventory spreadsheet provided as GFI and provide feedback. The estimated number of devices is 200 virtual servers, 122 physical servers and approximately 12-15 additional peripheral equipment such as storage and VTL.

- Provide information for all, (1) current server configurations, (2) network connectivity, and (3) current SAN and storage devices to include; specified communication ports on all servers/switches/security devices and VLANs & IPs schemas for inclusion into master documents being created/developed by the Government and its support contractor. The Contractor shall review and modify as required to provide the latest information on servers/switches/security devices, VLANs & IPs schemas including the 159,142 subnet. The Contractor shall track any additional changes to the Arlington data center until the move occurs.

- Review/validate/verify all documents provided as GFI pertaining to the FAS infrastructure. The Contractor shall review/validate/verify all documents provided as GFI pertaining to the FAS infrastructure that the Contractor currently supports including the 159.142 subnet and servers attached to it.

- Provide operational personnel (System administrators) for on-site support for the physical 'shut down' of all IT resources located in the CP4 data center. The Contractor shall also assist in providing the manpower for the physical, un-racking, racking of equipment. Note the move company will responsible for packing, moving, and unpacking equipment, not the Contractor. Assistance shall include assisting with the development of documentation that maps racks to devices, including bundling hardware, cables, etc. and for logically re-assembling in the Chantilly Data Center. The Contractor shall be responsible for powering down the systems at CP4. The Contractor shall assist with disconnecting and re-connecting the cables (power, internet, power) to the devices and also assist with the recording and the mapping of all cabling for re-assembly at the Chantilly site. The Contractor shall also conduct pre-coordination with the application owners, and submit appropriate CCB requests and associated paperwork. The Contractor shall assume that shutdown will occur the day prior to the move or at least adequate time will be allocated for a complete backup of the systems prior to the move.

- Provide operational support personnel (System administrators) for on-site support for the physical 'turn up' of all IT resources in Chantilly, VA data center after the Government and its support staff has moved the IT resources. The Contractor shall provide all support required to power up systems after the physical move is complete and equipment has been racked.

- Provide operational support personnel (Network Engineer) to provide on-site trouble shooting support in Chantilly, VA data center during the 'stand up' phase of the IT resources once they have been moved to Chantilly. Networking resources and System Administrators shall be on site to assist with the connectivity issues associated with the move. The Contractor shall create and document a priority listing of servers that need to be restored to service should issues arise during the move.

C.4.5 TASK 5 – PROVIDE CROSS FUNCTIONAL LIFE-CYCLE SERVICES

The contractor shall provide life-cycle technical support to GSA FAS business owners and applications teams for all infrastructure and hosting services. The contractor shall adhere to ITIL v3.0 best practices in performing work under this task. These cross functional life-cycle activities include, but are not limited to the following:

- Ensure compliance with GSA FAS policies, standards and regulations (Section J, Attachment Q) applicable to GSA FAS for information, information systems, personnel, physical and technical security;
- Develop and maintain a comprehensive Standards and Procedures Manual that contains the standards and procedures that will be used in the delivery of all Hosting Services;
- Conform to changes in laws, regulations and policies. Major Service Changes shall be proposed on a project-by-project effort basis to alter the environment to conform to the new requirements;
- Report performance against Service Level Requirements; and
- Provide timely creation, updating, maintenance and provision of all appropriate project plans, project time and cost estimates, technical specifications, management

documentation and management reporting in a form/format that is acceptable to GSA FAS for all Hosting Services projects and major Service activities.

C.4.5.1 SUBTASK 1 - PLANNING AND ANALYSIS

The contractor shall provide planning and analysis IT associated with researching new technical trends, products, and services, such as hardware components, and system Software~~, and Networks~~ that offer opportunities to improve the efficiency and effectiveness of FAS infrastructure support and Hosting Services. Planning and Analysis Services can also mitigate risks by reducing defects and improving the quality of IT services. The contractor's responsibilities include, but are not limited to the following:

- Participate in defining services and standards for Planning and Analysis activities;
- Perform technical and Service Planning and Analysis based on GSA FAS requirements (e.g., Availability, capacity, performance, backup and IT Continuity and Disaster Recovery Services);
- Provide recommendations for infrastructure and Services based on Planning and Analysis results;
- Continuously monitor technical trends through independent research; document and report on products and services with potential use for GSA FAS as they align with the GSA FAS business and technology strategies;
- Perform feasibility studies for the implementation of new technologies that best meet GSA FAS business needs and meet cost, performance and Quality objectives;
- Adhere to GSA FAS projects and SDLC requirements using Contractor's project management capabilities;
- Perform project management function for Contractor-managed projects as requested by GSA FAS;
- Participate in technical and business planning sessions to establish standards, architecture and project initiatives;
- Conduct regular planning for technology refreshes and upgrades; and
- Conduct technical reviews and provide recommendations for improvements that increase efficiency and effectiveness and reduce costs per the Planning and Analysis results

C.4.5.2 SUBTASK 2 - REQUIREMENTS DEFINITION

The contractor shall provide requirements definition services associated with the assessment and definition of functional, performance, IT Continuity and Disaster Recovery, and Security requirements that also comply with regulatory and GSA FAS policies. These requirements drive the technical design for the FAS environment. The contractor shall participate in defining requirements and standards, including appropriate requirements-gathering activities (e.g., focus groups, interviews). The contractor shall document requirements required to deliver services in agreed-to formats (e.g., system specifications, data models, upgrade requirements, transition requirements, network design schematics, etc.). The contractor shall ensure these requirements meet GSA-specific and Federal security policies. The contractor shall also define acceptance test criteria.

C.4.5.3 SUBTASK 3 - DESIGN SPECIFICATIONS

The contractor shall provide design specification services associated with translating user and information system requirements into detailed technical specifications. The contractor shall develop, document, and maintain Technical Design Plans and environment configurations based on GSA FAS design specifications, standards and requirements, including architecture, functional, performance, availability, maintainability, security and IT continuity, and disaster recovery requirements. The contractor shall determine and document required hosting services component upgrades, replacements and/or transition specifications (e.g., hardware, software, ~~networks~~). The contractor shall conduct site surveys for design efforts and document and deliver design specifications in a Design Specifications Document. The delivery dates of the Technical Design Plans and Design Specifications Document will be updated in the contractor's PMP.

C.4.5.4 SUBTASK 4 - ASSET MANAGEMENT

The contractor shall provide asset management services associated with ongoing management and tracking of new and upgraded hosting services components (e.g., hardware, Software, circuits) in the asset management system. The contractor's responsibilities include, but are not limited to the following:

- Deploy and manage an Asset Management system that meets GSA FAS requirements and adheres to defined policies;
- Provide GSA FAS inquiry and read access into the Asset Management System for all Assets;
- For GFP, input, maintain, update, track and report all in-scope Assets throughout the Asset life cycle (e.g., acquisition to retirement);
- For contractor-owned equipment, input, maintain, update, track and report all in-scope Assets throughout the Asset life cycle (e.g., acquisition to retirement);
- For GFP and Contractor-owned equipment, establish the Asset database to include, at a minimum, the following Asset information:
  - Manufacturer
  - Model
  - Serial number
  - Asset identification number
  - Asset location
  - Maintenance information and history including the age of the Asset
  - Warranty information
  - Transaction edit history (e.g., locations, billing and user)
- For contractor-owned equipment, perform ongoing physical Asset audit, in accordance with Asset Management Service Level Requirements, to validate that data in the database is accurate and current and GSA FAS has information that GSA FAS requires for internal chargeback systems;
- For contractor-owned equipment, perform ongoing physical Asset audit, in accordance with Asset Management Service Level Requirements, to validate that data in the database

is accurate and current and GSA FAS has information that GSA FAS requires for internal chargeback systems;
- For contractor-owned equipment, provide reports of Asset Management audit results; and
- For GFP and contractor-owned equipment, provide, upon GSA FAS approval, and implement an Asset Management Remediation Plan for Asset Management deficiencies

C.4.5.5 RESERVED

C.4.5.6 SUBTASK 6 - TRAINING AND KNOWLEDGE TRANSFER

The contractor shall provide Training and Knowledge Transfer services that consist of the following:

- Training for the improvement of skills through education for contractor employees on unique GSA FAS systems and software. The contractor shall participate in any mandatory, initial, and ongoing training provided by GSA FAS as required that would provide a learning opportunity about the GSA FAS business and technical environment.

The contractor shall develop, document, and maintain in the Standards and Procedures Manual training and knowledge transfer procedures that meet requirements and adhere to defined policies. The training program shall instruct GSA FAS personnel on the provisioning of contractor services (e.g., “rules of engagement,” requesting Services). The contractor shall develop, implement, and maintain a GSA FAS-accessible knowledge database/portal. The contractor shall develop and implement knowledge transfer procedures to ensure that more than one individual understands key components of the business and technical environment. The contractor shall participate in GSA FAS-delivered instruction on the business and technical environment.

The Government will not reimburse the contractor for training classes needed to remain current with systems, software, features, and functions.

C.4.5.7 SUBTASK 7 – MAINTENANCE AND BREAK/FIX SUPPORT

The contractor shall provide maintenance services associated with the maintenance and repair of hardware, software and networks to include "Break/Fix" services. Installed platform and product version levels are not to be more than one version behind the current commercial release, unless coordinated with GSA FAS architectural standards committee. The contractor’s responsibilities include, but are not limited to, the following:

- Develop, document and maintain in the Standards and Procedures Manual, Maintenance procedures that meet requirements;
- Develop Maintenance schedules;
- Ensure appropriate Maintenance coverage for all Hosting Services components for Contractor-owned equipment;

- Provide maintenance and Break/Fix support in GSA FAS defined locations, including dispatching repair technicians to the point-of-service location if necessary for Contractor-owned Equipment;
- For GFP and contractor-owned equipment, provide access to required hardware by Break/Fix personnel;
- For GFP and contractor-owned equipment, perform diagnostics and maintenance on Hosting Services components including hardware, Software, peripherals, Networks and special-purpose devices as appropriate;
- For GFP and contractor-owned equipment, install manufacturer field change orders, service packs, firmware and Software maintenance releases, etc;
- For GFP and contractor-owned equipment, perform product patch, "bug fix," service pack installation or upgrades to the current installed version;
- For GFP and contractor-owned equipment, perform maintenance-related software distribution and version control, both electronic and manual;
- Replace GFP and contractor-owned defective parts, including preventive maintenance, according to the manufacturer's published mean-time-between failure rates; and
- For GFP and contractor-owned equipment, conduct maintenance and parts management and monitoring during warranty and off-warranty periods.

The GFP provided at Task Order award and subsequent maintenance and/or licensing agreements shall convey to the contractor for annual renewals and management. A maintenance roster shall be maintained for the duration of the Task Order. Active maintenance and licensing agreements will be turned over to the Government at the completion of the task.

C.4.5.8 SUBTASK 8 - AVAILABILITY MANAGEMENT

The contractor shall provide availability management services to assist GSA FAS to plan, measure and monitor availability of the IT Infrastructure, services, and supporting Hosting Services organization. Availability management seeks to achieve, over a period of time, a reduction in the frequency and duration of incidents that impact availability. The Contractor shall continuously strive to improve availability to ensure the requirements are met consistently. Availability management includes the evaluation, design, implementation, measurement and management of the infrastructure availability from a component and an end-to-end perspective, including new or modified IT service management methodologies and tools, as well as technology modifications or upgrades of IT infrastructure systems and components. The contractor shall provide the following key availability management activities:

- Determine business unit availability requirements for new or enhanced Service and formulating the availability and recovery design criteria for the infrastructure to ensure Services are designed to deliver the appropriate levels of Availability;
- Determine the critical business functions and impact arising from IT component failure. Where appropriate, reviewing the availability design criteria to provide additional resilience to prevent or minimize impact to the business;
- Identify opportunities to optimize the availability of the infrastructure to deliver cost effective improvements that deliver tangible business benefits;

- Define the targets for availability, reliability and maintainability for the infrastructure components that underpin the service and ensure these targets are documented and agreed upon within SLRs, OLAs and contracts;
- Establish measurements and reporting of availability, reliability, and maintainability that reflect the business, stakeholder and IT support organization perspectives;
- Monitor and trend analysis of the availability, reliability and maintainability of systems and components;
- Review service, system and component availability, identifying unacceptable levels and ensuring appropriate corrective actions are taken to address availability shortfalls;
- Investigate the underlying reasons for unacceptable availability;
- Produce and maintaining a forward-looking Availability Plan that prioritizes and plans overall availability improvement; and
- Provide a range of availability reporting to ensure that agreed-upon levels of availability, reliability, and maintainability are measured and monitored on an ongoing basis

- The contractor shall also provide the following under this subtask: Develop Availability Management Policies and Procedures and determine appropriate Availability Management tools and methods that support GSA FAS Availability Management support requirements;
- Implement agreed-upon Availability Management policies and procedures and supporting processes;
- Provide unrestricted read access by GSA FAS-authorized staff and designated personnel to all current and historical Availability knowledgebase records;
- Participate in user requirements gathering and analysis when new IT systems and services are being defined to ensure that IT Services and systems are designed to deliver the required levels of Availability required by the business;
- Create Availability and recovery design criteria to be applied to new or enhanced Infrastructure design;
- Coordinate with the IT service support and service delivery management personnel from GSA FAS and third-party vendors to research, review and assess Availability issues and optimization opportunities;
- Participate and cooperate with GSA FAS in defining the Availability SLR measures and reporting requirements;
- Recommend appropriate tools and practices to measure and report on agreed-upon Availability SLRs for new and enhanced IT Infrastructure;
- Ensure that approved Availability SLR measurement tools and practices are implemented;
- Monitor and maintain an awareness of technology advancements and IT best practices related to Availability optimization and periodically provide updates to GSA FAS IT management;
- Ensure that all Availability Management improvement initiatives conform to defined Change Control procedures set forth in the Procedures Manual;
- Coordinate and take ownership of Availability Management across all Hosting Services service areas with GSA FAS and third parties (e.g., public carriers, Internet service providers, third party vendors, et. al.);

- Participate in Problem Management review sessions as appropriate, specifically those Problems related to outages of critical systems;
- Monitor actual IT Availability achieved versus targets and ensure shortfalls are addressed promptly and effectively;
- Conduct Availability Assessment review sessions and provide cost-justified improvement recommendations;
- Coordinate with GSA FAS and third-party service providers to gather information on IT systems and service availability issues and trends to be used for trend analysis;
- Produce and maintain a forward-looking Availability Plan which prioritizes and plans approved IT Availability improvements;
- Provide a range of IT Availability reporting to ensure that agreed levels of Availability, reliability and maintainability are measured and monitored on an ongoing basis.
- Promote Availability Management awareness and understanding within the IT support organization; and
- Perform regular reviews of the Availability Management process and its associated techniques and methods to ensure that all of these are subjected to continuous improvement and remain fit for purpose.

C.4.5.9 SUBTASK 9 - CAPACITY MANAGEMENT

The contractor shall perform capacity management services associated with ensuring that the capacity of the Hosting Services matches the evolving demands of GSA FAS business in the most cost-effective and timely manner. Capacity management encompasses the following:

- Monitoring of performance and throughput of IT Services and supporting IT components;
- Understanding current demands and forecasting for future requirements;
- Developing capacity plans which will meet demand and Service Level Requirements;
- Conducting risk assessment of capacity recommendations;
- Identifying financial impacts of capacity plans; and
- Undertaking tuning activities

The contractor shall perform the following:

- Develop, document and maintain in the Standards and Procedures Manual, Capacity Management Procedures that meet requirements;
- Establish a comprehensive Capacity Management planning process;
- Define, develop and implement tools that allow for the effective capacity monitoring/trending of IT infrastructure, applications and IT components;
- Continually monitor IT resource usage to enable proactive identification of capacity and performance issues;
- Capture trending information and forecast future GSA FAS capacity requirements based on GSA FAS-defined thresholds;
- Assess Incidents/Problems related to throughput performance;
- Recommend changes to capacity to improve service performance; and

- Maintain capacity levels to optimize use of existing IT resources and minimize GSA FAS costs to deliver Services at agreed-to Service Level Requirements.

C.4.5.10 SUBTASK 10 – PERFORMANCE MANAGEMENT

The contractor shall provide performance management services associated with tuning Hosting Services' components for optimal performance. The contractor shall monitor the various hardware and software components of the GSA FAS Open Systems processing environment for availability and potential error conditions.
The contractor shall collect performance metrics and monitor the performance of critical components such as servers, databases, and applications (where technically feasible) for Availability / Uptime, Response Time, End-to-end Throughput, and Bandwidth. The contractor shall report GSA FAS Open Systems availability, at the component level, on a monthly basis. This includes Performance Analysis and Performance Reporting as stated below:

- **Performance Analysis.** The contractor shall analyze performance metrics collected by the automated monitoring agents to track usage and trends. The contractor shall provide recommendations to maintain or improve performance.
- **Performance Reporting.** The contractor shall prepare and submit a Performance Report that charts the actual performance of the GSA FAS Open Systems processing environment within the reporting period against specific thresholds.

The contractor shall perform the following:

- Develop, document and maintain in the Standards and Procedures Manual, Performance Management procedures that meet requirements;
- Perform Hosting Services component tuning to maintain optimum performance in accordance with Change Management procedures;
- Manage Hosting Services component resources (e.g., devices and traffic) to meet defined Availability and performance Service Level Requirements;
- Provide regular monitoring and reporting of Hosting Services component performance, utilization and efficiency;
- Proactively evaluate, identify and recommend configurations or changes to configurations that will enhance performance;
- Develop and deliver improvement plans as required to meet Service Level Requirements.
- Implement improvement plans and coordinate with Third Parties as approved by GSA FAS; and
- Provide technical advice and support to the application maintenance and development staffs as required

C.4.5.11 SUBTASK 11 – SERVICE LEVEL MONITORING AND REPORTING

The contractor shall provide Service Level Monitoring and Reporting Services associated with the monitoring and reporting of service delivery with respect to infrastructure and hosting Service Level Requirements. The contractor shall report system management information (e.g.,

performance metrics and system accounting information) to the designated GSA FAS TPOC and COR representatives in a format agreed to by GSA FAS TPOC.
The contractor shall perform the following service level monitoring and reporting tasks:

- Develop, document and maintain in the Standards and Procedures Manual Service Level Monitoring and Reporting procedures that meet requirements and adhere to defined policies.
- Report on Service Level Requirement performance and improvement results.
- Coordinate Service Level Requirement monitoring and reporting with designated GSA FAS representative and Third Parties.
- Measure, analyze and provide management reports on performance relative to Service Level Requirements.
- Develop and deliver Service Level Requirement improvement plans where appropriate.
- Implement Service Level Requirement improvement plans.
- Provide GSA FAS portal access to performance and Service Level Requirement reporting and monitoring system.

C.4.5.12 SUBTASK 12 – INCIDENT MANAGEMENT

The contractor shall provide incident management associated with restoring normal service operation as quickly as possible and minimizing the adverse impact on business operations of GSA FAS, thus ensuring that the best possible levels of service quality and availability are maintained. While the incident management processes apply to level 1, level 2, and level 3 support groups, level 1 support is normally responsible for primary ownership of recording and tracking the incident and is responsible for the close coordination and ongoing monitoring and tracking of, and reporting on, Incidents that have been escalated to second-level and third-level support groups to ensure that escalated incidents are resolved as promptly as possible.
The contractor shall work within the *Information Technology Infrastructure Library (ITIL) version 3.0* framework and follow GSA FAS procedures for changes and incidents affecting any GSA FAS infrastructure.

The contractor shall provide the following incident management services:

- Incident detection and recording
- Incident classification and initial support
- Incident investigation and diagnosis
- Incident escalation
- Incident resolution and recovery
- Incident closure
- Incident ownership, monitoring, tracking, and communication

C.4.5.12.1 RESPONSE/SERVICE CENTER

The contractor shall provide a response/service center that supports telephonic and electronic mail submissions from designated FAS employees and applications support contractors. Problems may be identified by the contractor, FAS third parties, or by other FAS and GSA Help Desks. The contractor and FAS shall jointly develop a problem ticket notification process supporting notification to and from the GSA National Help Desk.

The contractor shall perform the following incident management tasks through the contractor's response/service center solution:

- Establish criteria for incident management support requirements, including equipment and services to be covered, Incident Severity level definitions and characteristics, incident classification and prioritization schema, escalation requirements, etc.
- Develop incident management policies and procedures that support GSA FAS incident management support requirements.
- Manage GSA FAS problem management system ticket queues related to the infrastructure.
- Provide, maintain, and manage an incident management system and knowledge database, including all hardware, software, databases, automated monitoring tools, and management and reporting tools, which are acceptable to GSA FAS.
- Provide unrestricted read access by GSA FAS-authorized staff and other personnel to all current and historical Incident records and knowledgebase data.
- Monitor the incident management system for automatically generated and logged incident alerts.
- Resolve Level 2 problems in accordance with the procedures manual, knowledge database documents, and configuration database(s).
- Identify and classify incident severity level characteristics and handle according to agreed-upon Incident response procedures.
- Escalate incidents to the appropriate next-level service group within contractor, GSA FAS, or third-party provider as soon as it is clear that the incident management technician is unable to resolve the incident without additional assistance, or as required, to comply with service level response times.
- Track incident resolution progress through to final closure and record/update incident record status as appropriate.
- Provide expert functional and process assistance for in-scope hosting services components at Level 2 or escalate to Level 3 resources as required.
- Provide Level 2 and Level 3 support for Applications Software on the supported applications list.
- Verify that all records (e.g., inventory, asset and configuration management records) are updated to reflect completed / Resolved Incident.
- Document solutions to resolved incidents in central knowledgebase. Accurately update all information pertinent to trouble ticket, including general verbiage, codes, et. al.
- Notify designated GSA FAS personnel of all Severity 1 and Severity 2 incidents.

- Maintain contractor-owned current and historical records of all calls and the resolution of those calls for the life of the contract and provide reporting and trend capabilities.
- For contractor-owned equipment, troubleshoot, diagnose and resolve incidents for all in-scope hardware and software warranty and non-warranty devices, including removing and / or repairing physically broken or inoperable devices.
- For contractor-owned equipment, coordinate dispatch for all in-scope devices and repair as required.
- Provide end-to-end incident identification, escalation and resolution management; and a closure process including those escalated to third parties.
- Determine wherever possible whether an incident should be treated as a problem (e.g., whether preventive action may be necessary to avoid incident recurrence) and, in conjunction with the appropriate problem management group, raise a problem record to initiate action.
- Determine wherever possible whether an incident should be treated as a problem (e.g., whether preventive action may be necessary to avoid Incident recurrence) and, in conjunction with the appropriate problem management group, raise a problem record to initiate action.
- Track ongoing status of any problem records to ensure that identified problems are addressed and resolved.
- Coordinate and take ownership of incident resolution across all hosting services service areas with GSA FAS and third parties (e.g., public carriers, Internet service providers, third party vendors, et. al.)
- Periodically review the status of Level 2 and Level 3 open, unresolved incidents and related problems and the progress being made in addressing problems.
- Participate in problem management review sessions as appropriate.
- Participate in incident review sessions.

C.4.5.12.2 PROBLEM MANAGEMENT SERVICES

The contractor shall provide problem management services to minimize the adverse impact of incidents and problems on the FAS business and to prevent incident recurrence by determining the root cause(s) and taking action to correct the situation. The contractor shall provide reactive problem management services by diagnosing and solving problems in response to one or more incidents that have been reported through incident management. The contractor shall also provide proactive problem management services to identify and solve problems and known errors before incidents occur. The contractor shall provide proactive problem management solutions to include performing predictive analysis activities, where practical, to identify potential future problems, develop recommended mitigation plans, and implement approved corrective mitigation actions and processes. The contractor shall maintain, update and disseminate information about problems and the appropriate workarounds and resolutions to ensure that the number and impact of incidents occurring within the GSA FAS IT infrastructure is reduced over time. The contractor shall perform the following key tasks included in problem management:

- Problem control
- Error control
- Proactive prevention of problems
- Identifying trends that could result in incidents or problems
- Performing major problem reviews
- Providing problem management reporting

The contractor shall provide problem management services for all identified problems that are determined to be related to IT systems and services under the control of contractor and within the scope of the task order. The contractor shall also provide coordination and assistance to GSA FAS and third-party vendors in performing their problem management Services. The contractor shall ensure resolutions to problems are implemented through the appropriate control procedures, especially change management and release management. The contractor shall coordinate problem management activities with the various teams within the contractor, GSA FAS and third-party vendors responsible for performing configuration management, availability management, capacity management, IT service continuity management, and service level management activities.

The contractor shall perform the following problem management services under this subtask:

- Participate in developing problem management requirements and policies.
- Participate in developing and implementing appropriate procedures and methodologies that support GSA FAS-approved problem management and Root Cause Analysis requirements and policies that comply with GSA FAS requirements.
- Establish and maintain a problem management knowledgebase where information about problems, root cause, known errors, workarounds and problem resolution actions are recorded and tracked. This knowledgebase may be the same knowledgebase as used by incident management.
- Provide GSA FAS access to problem management knowledgebase.
- Provide unrestricted read access by GSA FAS-authorized staff and other GSA FAS designated personnel to all current and historical Problem Management records and knowledgebase data.
- Ensure problem management activities conform to defined change control procedures set forth in the procedures manual.
- Coordinate with appropriate incident management teams and take ownership of problem management activities of all problems determined to reside in the contractor's service area of responsibility (e.g., detection, logging, Root Cause Analysis, et. al.)
- Coordinate, escalate and track problem management activities with GSA FAS and third parties related to problems determined to reside in all other IT infrastructure areas outside of the seat management area.
- Flag all incidents that require Root Cause Analysis (i.e., Severity 1 and Severity 2 incidents) per the agreed-to procedures.
- Ensure that recurring problems that meet defined criteria related to the contractor's IT service responsibility area are reviewed using Root Cause Analysis processes.

- Conduct proactive trend analysis of incidents and problems to identify recurring situations that are or may be indicative of future problems and points of failure.
- Track and report on problems and trends or failures and identify associated consequences of problems.
- Develop and recommend corrective actions or solutions to address recurring incidents and problems or failures, as well as mitigation strategies and actions to take to avert potential problems identified through trend analysis.
- Identify, develop, document, and recommend appropriate workarounds for known errors of unresolved problems and notify incident management and all other appropriate stakeholders of availability if approved.
- Coordinate and monitor status of Root Cause Analysis activities performed by GSA FAS and third-party vendors (e.g., from other IT service areas).
- Document and update problem management knowledgebase with information regarding problem resolution actions, activities and status (e.g., root cause, known errors, workarounds, etc.) and notify all appropriate stakeholders of availability of information.
- Coordinate with GSA FAS and third-party vendors to ensure that knowledge on problems related to other IT service areas is captured and entered into a centralized problem management knowledgebase.
- Ensure problem resolution activities conform to defined change control procedures set forth in the procedures manual.
- Provide status reports detailing the root cause of and procedure for correcting recurring problems and Severity 1 and Severity 2 incidents until closure as determined by GSA FAS.
- Participate in problem management review meetings and review and approve recommendations for actions, where appropriate.
- Periodically review the state of open Incidents and related problems and the progress being made in addressing problems.
- Create request for change documentation with recommended corrective actions to be taken to resolve a problem and submit to change management for review and approval.
- Provide problem management reporting as required.

C.4.5.13 SUBTASK 13 – CONFIGURATION MANAGEMENT

The contractor shall perform configuration management services associated with providing a logical model of the hosting services by identifying, controlling, maintaining and verifying installed hardware, software and network versions. The goal of configuration management is to account for all IT assets and configurations, provide accurate information on configurations and provide a sound basis for incident, problem, and change and release management and to verify configuration records against the infrastructure and correct any exceptions. The contractor shall propose, procure, implement, and maintain all needed automated tools (CMDB) and procedures, to implement the configuration management / administration process in a cost effective manner. The contractor shall have demonstrated expertise and knowledge of the proposed CMDB tool and have proven successful vendor relationships. The CMDB tool shall provide, at a minimum, the following features:

- Automated License management
- Patch management and automation
- Port enabling/disabling
- Automated server provisioning (both physical and virtual)
- Solaris and Linux server elements configuration "discovery" ability
- Interactions between infrastructure components

The contractor shall be prepared to demonstrate to the GSA FAS TPOC and GSA FAS management capabilities and demonstrations of the CMDB tool. The contractor shall be responsible to perform the following configuration management tasks:

- Define configuration management requirements and policies.
- Develop, document and maintain in the Standards and Procedures Manual configuration management procedures that meet requirements and adhere to defined policies.
- Establish configuration management database, in accordance with GSA FAS requirements.
- Select, install and maintain configuration management tools.
- Enter/upload configuration data into configuration database.
- Establish process interfaces to incident and problem management, change management, technical support, maintenance and asset management processes.
- Establish appropriate authorization controls for modifying configuration items and verify compliance with software licensing.
- Establish guidelines for physical and logical separation between development, test and production and the process for deploying and back-out of configuration items.
- Establish configuration baselines as reference points for rebuilds, and provide ability to revert to stable configuration states.
- Establish process for verifying the accuracy of configuration items, adherence to configuration management process and identifying process deficiencies.
- Provide GSA FAS configuration management reports as required and defined by GSA FAS.

C.4.5.14 SUBTASK 14 – CHANGE MANAGEMENT

The contractor shall provide change management services to include all activities to ensure that standardized methods and procedures are used for efficient and prompt handling of all changes. The goal of change management is to minimize the impact of change upon service quality and consequently to improve the day-to-day operations of the GSA FAS systems. Change Management covers all aspects of managing the introduction and implementation of changes affecting all hosting services and in any of the management processes, tools, and methodologies

designed and utilized to support the hosting services components. Change management processes are complementary to release management and configuration management, as well as incident management and problem management. The contractor shall work within the *Information Technology Infrastructure Library (ITIL)® version 3.0* framework and follow GSA FAS procedures for changes and incidents affecting any GSA FAS system. The contractor shall perform the following key change management tasks under this subtask:

- Request for Change (RFC) process
- Recording/Tracking process
- Prioritization process
- Responsibility assignment process
- Impact/Risk assessment process
- Establish and manage the schedule of approved changes
- Determine metrics for measuring effectiveness of a change
- Review / Approval process
- Implementation process
- Verification (test) process
- Closure process
- Participation in IT service continuity and disaster recovery planning
- Integrate with GSA FAS change management policies, procedures, processes and training requirements per the change management process components outlined above, including Change Control Board (CCB) composition, activities and the financial, technical and business approval authorities appropriate to GSA FAS IT and business requirements.
- Receive and document all Requests for Change (RFC) and classify proposed changes to the Services, which shall include change cost, risk impact assessment, and system(s) security considerations.
- Ensure that appropriate back-out plans are documented and in place in the event of systems failure as a result of the change.
- Provide change management plan to GSA FAS for review.
- Develop and maintain a schedule of planned approved changes (Forward Schedule of Changes or FSC) and provide to GSA FAS for review.
- Determine change logistics.
- Provide change documentation as required, including proposed metrics as to how effectiveness of the change will be measured.
- Participate in CCB meetings as GSA FAS deems appropriate or necessary.
- Oversee the approved change build, test, and implementation processes to ensure these activities are appropriately resourced and completed according to Change schedule.
- Ensure that thorough testing is performed prior to release and assess GSA FAS business risk related to any change that is not fully tested prior to implementation. (Submit a test plan for GSA FAS approval prior to the start of test.)
- Monitor changes, perform change reviews and report results of changes, impacts, and change effectiveness metrics.
- Verify that change met objectives based upon predetermined effectiveness metrics and determine follow-up actions to resolve situations where the change failed to meet objects.

- Close out RFCs that met any successful met change objectives or changes that were abandoned.

C.4.5.15 SUBTASK 15 – RELEASE MANAGEMENT

The contractor shall provide release management services that track changes to contractor-managed software and components that are required to support the infrastructure (e.g., virus detection software, software required to manage the SAN, backup software, retention of prior versions of production OS , etc.) release management activities take a holistic view of a change to a service, including all aspects, technical and non-technical, software, hardware and network changes. These changes can be implemented by rolling out a combination of new applications, infrastructure software, upgraded or new hardware, or simply by making changes to the service hours or support arrangements. Release management processes and activities are complementary to those of change management, configuration management, and problem management. Releases typically consist of a number of problem fixes and enhancements to an existing service. A release consists of the new or changed software required and any new or changed hardware needed to implement the approved changes. Releases are generally divided into the following categories:

- Major software releases and hardware upgrades or replacements, normally containing large areas of new functionality. A major upgrade or release usually supersedes all preceding minor upgrades, releases and emergency fixes.
- Minor software releases and hardware upgrades, normally containing small enhancements and fixes, some of which may have already been issued as emergency fixes. A minor upgrade or release usually supersedes all preceding emergency fixes.
- Emergency software and hardware fixes, normally containing the corrections to a small number of known problems.

The contractor shall provide the following key release management services:

- Establish standardized release management policies and procedures.
- Manage Release Planning and Scheduling for overall the release schedule, as well as individual Releases.
- Establish and managing a release documentation and identification schema.
- Manage the release design, build, and configuration processes.
- Release testing and testing management.
- Rollout planning including quality plans and back-out plans.
- Release communication, preparation, and training.
- Manage the successful rollout/distribution and installation of all elements of a release.
- Ensure that only correct, authorized, and tested versions are installed and that changes are traceable and secure.
- Document each release and update the CMDB.

- Recommend release management policies, procedures, processes, and training requirements per the release management process components outlined above.
- For Contractor-owned equipment, establish and maintain an appropriate secure environment(s) where all authorized versions of all hardware spares (Definitive Hardware Store or DHS) are stored and protected.
- For Contractor-owned equipment, ensure that all hardware spares are secured in the DHS and update configuration database(s).
- Establish, manage, update and maintain the overall release plan and release schedule for all planned releases.
- Establish and administer the version control schema as it relates to release management of GSA FAS custom applications.
- Develop, manage, update and maintain formal release plans for each release in coordination with change management.
- Develop quality plans and back-out plans as appropriate for each Release.
- Provide release management plans and schedules to GSA FAS for review.
- Conduct site surveys, as necessary, to assess existing software being used to validate Release package requirements and dependencies.
- For Contractor-owned equipment, conduct site surveys, as necessary, to assess existing hardware being used to validate release package requirements and dependencies.
- Plan resource levels and requirements for supporting a release.
- Ensure that any new software or support services required for the release are procured and available when needed.
- For contractor-owned equipment, ensure that any new hardware required for the Release is procured and available when needed.
- Ensure that all necessary testing environments are available and properly configured to support release testing.
- Schedule and conduct release management meetings to include review of planned Releases and results of changes made.
- Identify and document all Configurable Items (CIs) that need to be included in the Release, as well as all system inter-dependencies.
- Plan and manage the acceptance testing process for each release.
- Provide Release documentation as required.
- Review release management details and alter as appropriate to meet the needs of the GSA FAS (e.g., back out plan, go/no go decision).
- Notify GSA FAS affected applications “owners” of release timing and impact.
- Implement release in compliance with change management requirements and adherence to detailed release plans.
- Modify configuration database, asset management items, and service catalog (if applicable) to reflect changes to CIs due to the release.
- Conduct post-mortem of releases that necessitated implementation of the back-out plan and develop and implement appropriate corrective or follow-up actions to minimize future occurrences.

C.4.5.16 SUBTASK 16 – PROVIDE CONTINUOUS IMPROVEMENT CONSULTING

The contractor shall provide continuous improvement consulting services to the FAS OCIO to enable GSA FAS to reach new levels of performance while reducing costs. In partnership with the FAS OCIO, the contractor shall recommend processes and technology improvements (tools, processes, methodologies, etc.) that will increase efficiency and enable FAS to continue to provide best value services to FAS clients. The contractor shall identify improvements and establish a baseline as a benchmark for metrics. After approval by the FAS OCIO TPOC or designee, the contractor shall implement support recommendations and track the progress by capturing metrics against projected improvement. The contractor shall report on performance of implemented support improvements, issue reports on IT service area performance, and identify possible product enhancement opportunities for improved performance and potential cost savings. The contractor shall also record implemented improvements through the FAS OCIO-approved Change Control process.

C.4.6 TASK 6 – PROVIDE INFRASTRUCTURE MODERNIZATION PLANNING AND IMPLEMENTATION (Optional Task)

As a technology leader in the Federal Government space, GSA FAS is aware of, and impacted by, the ever increasing costs relating to growth of data and the hardware and network costs. GSA FAS recognizes the most recent industry advances and growing maturity in hosting services for offerings such as public and private cloud computing and managed co-location, among other emerging technologies. The contractor shall propose a solution that would allow GSA FAS to move smaller, moderate, or larger portions of the current server and storage environment, as well as any additional applications GSA FAS develops or becomes responsible for; to one or a combination of these hosting paradigms, with the physical move starting not later than Option Year 2.

The contractor may suggest single, combinations, or alternative approaches to the above components, while remaining focused on mitigating risk to the overall GSA FAS environment. GSA FAS seeks to provide a technical framework to enable rapid response to emerging Internet trends and complex Government needs. GSA FAS is seeking to evaluate, test, and adapt legacy applications through the use of cost-effective technologies like virtualization, cloud computing and IaaS. It is the Government's goal to migrate small, low-risk applications to one or more hosting paradigms. Upon successful implementation and acceptance by the Government, additional applications will be considered for migration to this hosting paradigm. GSA FAS will require computing resources which are comparable too, or greater than FAS GFP equipment.

Initial components under consideration to be migrated by GSA FAS include:

- Web server layer to private cloud / managed co-location
- Network / server / storage to private cloud / managed co-location
- Migration of Development, Test and production environments to a virtualized infrastructure and/or IaaS or Cloud/Emerging
- Backup as a Service / Enhanced Backup Processes
- Enhanced Disaster / Business Recovery solution

The Government requires disposition of equipment either in trade or disposal (within GSA standard procedures), or equipment to be repurposed based on government direction of servers as applications are moved from GFP Hosting Environment to the Task 6 IaaS solution.

C.4.6.1 SUBTASK 1 - VIRTUALIZED DEVELOPMENT, TEST AND PRODUCTION ENVIRONMENTS

GSA FAS intends to transition to a technical framework that is more cost-effective and can be easily adapted to meet the complex needs of the organization. GSA FAS seeks to utilize a virtualized environment for a number of applications in the environment. The contractor shall propose and implement a Transition Plan for the Test, Development, and Production environments to migrate to a virtualized environment. This transition is part of an ongoing effort for GSA FAS to identify and consolidate candidate servers and applications in the FAS environment. FAS will identify low-risk applications that are suitable for virtualization and/or IaaS.

C.4.6.1.1 GENERAL VIRTUALIZATION SERVICES REQUIREMENTS

The contractor shall provide a cost effective, virtualization solution that utilizes proven and stable virtualization technologies. The contractor shall provide the following:

- Use industry standard techniques to determine which servers are candidates for virtualization. This may include CPU utilization, performance requirements of hosted applications, memory utilization of specific servers, etc.
- Work with GSA FAS and application owners to deliver a proposed migration plan for all identified servers approved for migration.
- Implement a migration plan for the development and test environment servers while mitigating risk for application development.
- Present cost proposal and license procurement details for virtualization.
- Procure all items required for migration and implement based on GSA FAS approved migration plan.
- Provide documentation of compliance with appropriate industry standards as applied to the proposed hosted solution.
- Adhere to the GSA FAS backup policy and ensure that backups are completed in accordance with GSA FAS requirements.
- Adhere to the GSA FAS security policy and ensure that all virtualized hosts and/or GFP equipment is hardened in accordance with these standards.
- GSA FAS shall retain ownership of all virtual machines, templates, clones and scripts / applications created with this SOW and maintain the right to request full copies of virtual machines at any time.
- GSA FAS shall retain ownership of all software installed on virtual machines and any application or product that is developed under the SOW.

C.4.6.1.2 VIRTUAL INFRASTRUCTURE REQUIREMENTS

The contractor shall provide the following virtual infrastructure services to FAS OCIO:

- Provide centralized management of virtual resources.
- Provide the capability to report real-time usage metrics to include CPU, memory, disk and network usage.
- Provide support for virtual machines running Linux and Solaris.
- Provide the capability to dynamically reallocate virtual machines based on load, with no service interruption.
- Provide the capability to create virtual machine templates.
- Provide the capability to copy or clone virtual machines for archiving, troubleshooting and testing.
- Provide multiple network switches to allow for network fault tolerance.
- Provide the ability to project capacity growth based on forecasting and trending.
- Provide self-service capabilities to allow GSA FAS CIO staff to create new virtualized instances.

C.4.6.1.3 VIRTUALIZATION HYPERVISOR REQUIREMENTS

The contractor shall provide virtualization hypervisor services to include the following:

- Provide virtualization capabilities based on the x86 processor architecture and meet all three of the following criteria (a, b, and c):
  - Virtual host processors shall be a minimum of 3GHz.
  - Virtual host processors shall be of the same manufacturer, model and stepping.
  - Virtual host processors shall support 64bit operations.
- Provide support for virtual machines with memory requirements up to and including 16GB.
- Provide support for multiple processor virtual machines.

C.4.6.1.4 VIRTUALIZATION STORAGE REQUIREMENTS

The contractor shall provide the following virtualization storage consulting services:

- Provide high availability, centralized network accessible storage.
- Provide the ability to snapshot virtual machines.
- Provide adequate flexibility for adding additional capacity.
- Provide the ability to scale across multiple physical sites.

C.4.6.2 SUBTASK 2 – BACKUP AS A SERVICE / ENHANCED BACKUP PROCESSES

GSA FAS's strategic goal is to migrate away from tape-based backup and optimize the existing backup process to enable effective handling of retention policies and access to information. Under this subtask, the contractor shall propose, procure, and implement as operational, a backup solution to address the following requirements.

C.4.6.2.1 BACKUP AS A SERVICE / ENHANCED BACKUP REQUIREMENTS

The contractor shall ensure that all systems in the scope of this task order be backed up with an industry standard solution that allows for the following:

- Improved speed of restoration and self-service capabilities for GSA FAS application teams' on-demand restores of data
- Ongoing data storage
- Daily incremental and weekly full backups
- Backup on media appropriate for long-term off-site storage
- Backup of virtual machine files
- Administer, maintain and test all virtual machine and system backups in accordance with GSA standards
- Backups shall be stored in a secure off-site location with weekly transfers from host to storage site on a 6-month rotation schedule
- Annual permanent backups will be retained with the first full backup serving as the first annual backup and the anniversary date for permanent backups

C.4.6.3 SUBTASK 3 – ENHANCED DISASTER/BUSINESS RECOVERY

The contractor shall propose and test a comprehensive disaster / business recovery solution. The contractor shall prepare an Enhanced Disaster/Business Recovery Plan at a level of detail as mutually agreed on by the GSA FAS TPOC and the contractor. The GSA FAS TPOC shall review the plan and, once approved by the GSA FAS TPOC and COR, the Enhanced Disaster/Business Recovery Plan shall be updated quarterly to guide future open systems infrastructure improvements. The proposed solution may utilize a dedicated or a shared infrastructure running virtual servers.

C.4.6.3.1 ENHANCED DISASTER / BUSINESS RECOVERY REQUIREMENTS

The contractor's proposed solution shall incorporate the technical requirements set forth in Section C.4.3.3 of the PBSOW and address the following:

- The ability to failover and become the primary site should a disaster occur
  - The ability to failover shall be tested at minimum of once a year
- Geographically separate disaster recovery environments
- The ability to migrate or move virtual machines whether online or offline from the primary site to the secondary site.
- Business recovery site(s)
- Open systems processing configurations
- Open systems network connectivity
- Business recovery notification
- Business recovery process
- Business recovery support
- Business recovery testing

C.5 SECTION 508 COMPLIANCE REQUIREMENTS

Unless the Government invokes an exemption, all EIT products and services proposed shall fully comply with Section 508 of the Rehabilitation Act of 1973, per the 1998 Amendments, 29 U.S.C. 794d, and the Architectural and Transportation Barriers Compliance Board's Electronic and Information Technology Accessibility Standards at 36 CFR 1194. The contractor shall identify all EIT products and services proposed, identify the technical standards applicable to all products and services proposed and state the degree of compliance with the applicable standards. Additionally, the contractor must clearly indicate where the information pertaining to Section 508 compliance can be found (e.g., Vendor's or other exact web page location). The contractor must ensure that the list is easily accessible by typical users beginning at time of award.