

**Performance Work Statement  
for the  
General Services Administration  
Office of the Chief Information Officer (OCIO)  
GSA Infrastructure Technology  
Global Operations  
General Cross-cutting  
Client Order ID Numbers:  
A06S47T0040 & 9T8NDWIS002  
Revised January 26, 2010**

- 1. **Background** ..... 1
- 2. **Objective** ..... 2
- 3. **Scope**..... 2
- 4. **Critical GSA Task Order Roles**..... 3
- 5. **Performance Metrics** ..... 3
- 6. **Place of Performance**..... 4
- 7. **Work Schedule**. .... 4
- 8. **Government Furnished Resources and Equipment**..... 4
- 9. **Security Requirements** ..... 4
- 10. **Key Personnel**..... 6
- 11. **Removal of Contractor Personnel**. .... 6
- 12. **Travel** ..... 6
- 13. **Training** ..... 6
- 14. **Government Work Force** ..... 7
- 15. **Standardized Enterprise Resource Management (ERM) Framework** ..... 7
- 16. **Access to the Standardized ERM Framework** ..... 9
- 17. **Task Order Management** ..... 9
- 18. **Task Order Responsibilities Common to all Sub-Tasks** ..... 10
- 19. **Communications and Deliverables**..... 13
- 20. **Section 508 Compliance**..... 19
- Appendix A Sub-Task A - Program Management**..... A-1
- Appendix B Sub-Task B - Client Management Services**..... B-1
- Appendix C Sub-Task C - Consolidated Enterprise Help Desk**..... C-1
- Appendix D Sub-Task D - Local Support Services**..... D-1
- Appendix E Sub-Task E - Network Operations**..... E-1
- Appendix F Acronym Dictionary** .....F-1
- Appendix G Table of Attachments**..... G-1

## **1. BACKGROUND**

- 1.1.** In January 2005, GSA announced that the Federal Technology Service and Federal Supply Service would be consolidated into a single organization, the Federal Acquisition Service (FAS). GSA recently received official approval of the Federal Acquisition Service plan from the House and Senate Appropriations Committees. The goal of the plan is create a more effective and efficient agency that will enhance our ability to deliver goods and services at best value, improve GSA's capacity to anticipate customer needs, and sharpen our focus on providing expert solutions. In addition to the creation of FAS, the reorganization plan includes changes in GSA IT infrastructure operations across all of GSA.
- 1.2.** Historically at GSA, the Office of the Chief Information Officer (OCIO), has managed the Agency's wide area network and electronic messaging system but each of the three major Services has been responsible for managing its own desktop support, server support, helpdesk support, etc. The Public Building Services' (PBS) and the Federal Technology Services' (FTS) IT infrastructure is supported locally where each of the eleven regions operate their own IT services and support with a degree of autonomy. Federal Supply Service (FSS) operates its infrastructure on a centralized model. In other words, where PBS and FTS may use a different support vendor and have several service levels associated with each region, FSS uses a single contract and set of service levels to operate with a high level of standardization across the GSA enterprise.
- 1.3.** A major component to making GSA's information technology operation more efficient is centrally managed infrastructure operations. In addition to standardizing our operations across geographic and organizational boundaries, GSA expects to transform the operational dynamics of the existing organization. This transformation will include changes in GSA's organizational structure, contract management, operational processes and functional alignment. A goal of transformation is streamlining of operations to eliminate functional/organizational stovepipes while improving reliability of operations or levels of service.
- 1.4.** Infrastructure operations provide desktop support to approximately 15,000 GSA employees and contractors deployed around the world. Reliable and responsive service as well as quality hardware and software provide employees and contractors with the tools necessary to perform their jobs effectively.
- 1.5.** GSA uses legacy product sets to assist with managing its infrastructure. Approximately 75 percent of GSA utilizes Computer Associates (CA) Unicenter product set to support asset management, ticket processing, remote control, and automated software deployment. However, administration of the Unicenter product set is decentralized at the regional level. The remaining 25 percent primarily utilize a multi-vendor product set. The product set consists of Proxy remote control, WinInstall Asset Management, WinInstall Software Distribution Management and Remedy Helpdesk.

## **2. OBJECTIVE**

- 2.1.** The overall objective of this task order is to establish and sustain effective and efficient managed life cycle support of GSA's IT Infrastructure services. Through this task order, GSA will realize the benefits of consolidation and superior service levels for our customers. GSA wishes to implement an IT infrastructure that is consistent with industry best practices and expects the Contractor to provide a comprehensive solution for delivery and continuous improvement of infrastructure technology services. This will allow GSA to reap significant savings and improvements such as:
- 2.1.1. Achieve greater return on IT investment.
  - 2.1.2. Achieve consistent IT service delivery.
  - 2.1.3. Improve asset utilization.
  - 2.1.4. Provide an enterprise view of IT.
  - 2.1.5. Strengthen and standardize IT management within the Agency.
  - 2.1.6. Increase security posture.
- 2.2.** GSA's objective is to refresh workstations every three years, servers every 3 to 4 years, and WAN/LABN every 5 years subject to budget availability.

## **3. SCOPE**

- 3.1.** The Government will obtain information technology infrastructure support services and the Contractor shall perform support services including, but not necessarily limited to, the following areas:
- 3.1.1. Program Management Services (see Appendix A)
  - 3.1.2. Client and Server Management Services (see Appendix B)
    - 3.1.2.1. Collaboration
      - 3.1.2.1.1. Client/Remote Mail
        - 3.1.2.1.1.1. Client Deployment Services
      - 3.1.2.1.2. Groupware
      - 3.1.2.1.3. Directory Management Services
    - 3.1.2.2. Desktop Management Services
      - 3.1.2.2.1. Software Deployment
      - 3.1.2.2.2. Client Engineering Services
      - 3.1.2.2.3. Server Services
  - 3.1.3. Consolidated Enterprise Helpdesk Services (see Appendix C)
    - 3.1.3.1. Customer Service & Support
  - 3.1.4. Local Support Services (see Appendix D)

- 3.1.5. Network Operations (see Appendix E)
  - 3.1.5.1. Voice and Data Communications Services
    - 3.1.5.1.1. Wide Areas Network Services
    - 3.1.5.1.2. Internetworking and Security Services
    - 3.1.5.1.3. Network Operations Center Services
    - 3.1.5.1.4. Voice and Video Services
    - 3.1.5.1.5. Remote Mobile Technologies
  - 3.1.6. Security
  - 3.1.7. Earned Value Management
- 3.2. The Contractor shall manage the work performed under the task order by using the Information Technology Infrastructure Library (ITIL) framework.

#### **4. CRITICAL GSA TASK ORDER ROLES.**

GSA will designate one or more individuals to perform each of the following roles in support of the task order and its sub-tasks:

- 4.1. GSA Program Manager (GSA PM). Responsible for the overall direction of the task order, and the final authority for all management direction. Provides guidance and direction to all Government IT staff supporting the task order, and helps assure timely response to contractor requests for needed Government information and services.
- 4.2. GSA Contracting Officer (GSA CO). Responsible for all task order administration and task order directives. This individual is empowered by GSA to legally bind GSA and provide needed direction. This individual is the only GSA employee with authority to make financial commitments for the Government or change any task order terms and conditions.
- 4.3. GSA Contracting Officer's Representative (GSA COR). The COR is responsible for overall task order administration including the approval of task order invoices and vendor evaluation. Because of the complexity of this task, the COR will be supported by multiple GSA COTRs.
- 4.4. GSA Contracting Officer's Technical Representative (GSA COTR). Responsible for day-to-day administration, monitoring of the progress and vendor performance, technical evaluation of deliverables, provide technical interpretation of the requirements and general coordination with GSA staff and resources for accomplishment of the requirements.

#### **5. PERFORMANCE METRICS**

Performance metrics for this task order are presented in Attachment 18. GSA may choose to revise these metrics based on experience gained, contractor performance, and/or GSA requirements. Performance metric changes will be mutually negotiated between GSA and the Contractor. The incentive fee structure and metrics are included as Attachment 26.

## **6. PLACE OF PERFORMANCE.**

Unless otherwise specified in a sub-task, work will normally be performed at Government owned or leased facilities in the locations found in Attachment 2 or commercial locations as directed by the Government. The Contractor shall obtain prior written approval from the CO to work in any location outside of standard Government facilities.

## **7. WORK SCHEDULE.**

Unless otherwise provided for in a sub-task, the Contractor shall report to work Monday through Friday, excluding Federal Holidays, starting no earlier than 6:00 am, local time and ending no later than 7:00 pm local time. No overtime rates will be paid.

## **8. GOVERNMENT FURNISHED RESOURCES AND EQUIPMENT.**

- 8.1.** Government Furnished Resources (e.g. office space, computers, desks, landline phones, fax, copier, standard office supplies) will normally be provided at a Government owned or leased facility, unless otherwise specified in the sub-task.
- 8.2.** The Contractor and any employee or consultant of the Contractor is prohibited from using U.S. Government resources for any purpose except as specifically described in the specific task order and related to a sub-task.
- 8.3.** The government requires a standardized ERM framework. The government owns licenses for software it currently uses to support those functions. The Contractor shall use a standardized ERM framework as part of its service. The Contractor does not need to use any of the software the government currently uses to support those functions. However, if the Contractor is interested in reducing its proposed costs, it may leverage software licenses owned by the government. The government will furnish licenses identified in Attachment 22.

## **9. SECURITY REQUIREMENTS**

Security Clearances – The Contractor shall provide personnel with appropriate clearances and background checks. At a minimum, these checks shall be consistent with the requirements of HSPD 12 as stated in GSA’s “Standard Operating Procedure for GSA HSPD-12 Personnel Security Process.” The results of these clearances shall be provided to the Federal Government ISSM or ISSO upon request, but consistent with maintaining privacy of the individuals. Briefly GSA’s guidance states:

- 9.1.** Contract employees must have a National Agency Check with written Inquiries (NACI); National Agency Check with written Inquiries and Credit (NACIC) for contract employees; or equivalent investigation initiated. Successful results from the FBI National Criminal History Check (i.e. fingerprint check) portion of the NACI/NACIC must be received for issuance of an identity credential for access to GSA facilities and IT systems.
- 9.2.** Subject to the requirements of GSA’s “Standard Operating Procedure for GSA HSPD-12 Personnel Security Process,” 75% of all contractors must have, at minimum, a NACIC in accordance with the accepted Transition Plan. The remaining 25% must submit NACIC paperwork (which includes a fingerprint check) forms two

weeks prior to start date so that they will have a favorable fingerprint check before beginning work. Those receiving favorable results from the fingerprint check will be granted limited access only until the favorable NACIC's are complete. At the discretion of the Government, higher levels of clearance may be required for certain positions

- 9.3.** Badges - Employees working at a Government facility may be required to display, on their person, a Government-provided identification badge, that will include the full name of the employee and the legal name under which the Contractor is operating. The identification badge numbers and data will be kept in a Government-maintained computer database for security purposes. The Contractor shall return all badges to the Government program manager, or designee, on the same day an individual's employment is terminated and/or upon termination of the task order. The Contractor shall notify the Government program manager, or designee, immediately of any lost badges.
- 9.4.** Data Security - Contractor staff may have access to privileged and confidential materials of the United States Government. These printed and electronic documents are for internal use only and remain the sole property of the United States Government. Some of these materials are protected by the Privacy Act of 1974 (AMENDED) and Title 38. Unauthorized disclosure of Privacy Act or Title 38 covered materials is a criminal offense. Each Contractor employee will be given access to only the information and facilities needed to perform the work associated with the task order.
- 9.5.** System Security: The Contractor(s) shall comply with all the physical and data security policies in effect at GSA. Copies will be made available as part of the task order placement process. The Contractor shall participate in security functions relevant to the tasks being performed that may include Security Safeguard Reviews, audits, reporting suspected security violations, acting to secure system environments, responding to computer security alerts and any other review or actions required to ensure computer systems are not violated or vulnerable. The Contractor shall coordinate and assist with processing responses to periodic security scans. The responses include, but are not limited to, identifying false positives, applying patches, hot fixes, upgrades and forwarding vulnerability assessment information to system owners. This may also include physical security as authentication devices are deployed for access control to Government-controlled space occupied by GSA employees and employees of tenant agencies.
- 9.6.** Interconnection Agreements – Where the infrastructure must be connected to other third party capabilities, the Contractor shall cooperate in good faith in the development and implementation of interconnection agreements as appropriate. Interconnection agreements are required whenever the infrastructure has an automated and interactive connection with another infrastructure. Links, search bots, pushing out files, etc. are not considered automated and interactive connections.

## **10. KEY PERSONNEL**

- 10.1.** Due to the complexity, sensitivity and high-level visibility of this task order, the Government requires the Contractor to submit in ITSS a statement of qualifications for each key personnel prior to the individual's commencing work. The Contractor shall provide the COR ten (10) working days advance notification of key personnel changes. In the event that named key personnel in the Contractor's proposal are unable to perform their duties, the Contractor shall submit a replacement statement of qualifications to the COR to minimize any impact to task order performance.
- 10.2.** In the event of any key personnel absence, which exceeds five working days, the Contractor will provide a qualified individual on an interim basis until the replacement key personnel is available, unless the interim staffing is waived by the COR. All proposed substitutes shall have qualifications equal to or higher than the qualifications of the person to be replaced.
- 10.3.** The results of these evaluations will be promptly provided to the Contractor through ITSS. The CO will make a final determination of acceptability and if the proposed individual is found to be unacceptable, the Contractor will supply another substitution within 15 calendar days.

## **11. REMOVAL OF CONTRACTOR PERSONNEL.**

Due to the complexity, sensitivity and high-level visibility of the work required under this task order, the CO reserves the right to request the removal of personnel, including sub-contractor(s), at any time during the life of the task order due to security violations or exhibiting non-professional behavioral problems. The Contractor shall provide a qualified replacement(s) within ten (10) working days.

## **12. TRAVEL**

Contractor personnel may be directed to travel to Government installations, commercial facilities, OCONUS, and other offsite locations in performance of duties. The COTR will determine specific location, duration and number of travelers to meet mission needs. Travel inside the 50-mile radius from their duty station will not be separately reimbursed. All travel will be reimbursed in accordance with the Federal Travel Regulation (FTR). The estimated ceiling amounts for travel costs are included in the task order SF1449 CLIN structure.

## **13. TRAINING**

- 13.1.** The Contractor shall provide fully trained and experienced personnel required for performance of all work under this task order. Training of contractor personnel to fulfill these requirements shall be performed at the Contractor's expense. The Contractor shall provide training for contractor employees within a reasonable amount of time after issuance of software upgrades.
- 13.2.** Training at Government expense will not be authorized for replacement personnel or for the purpose of keeping contractor personnel abreast of advances in the state-of-the-art or for training contractor employees on equipment, computer languages, and computer operating systems that are available on the commercial market. Training shall not be authorized at Government expense to develop skills on hardware and/or

software that were already in use by the Government at the time of the award of the task order.

- 13.3. GSA may fund training uniquely related to GSA/Government information infrastructure environment or general work environment with the prior approval of the COR. The estimated ceiling amounts for training costs are included in the task order SF1449 CLIN structure.

#### **14. GOVERNMENT WORK FORCE**

- 14.1. The Government currently has federal staff performing functions, which must interface with those functions, which the Contractor is expected to perform. The Government understands that this working environment presents challenges but that these challenges are not insurmountable. In order to facilitate the efficient progress of the work, the Government offers the following principles, which will be used to guide the workflow.

- 14.1.1. The Contractor will have full authority over any work assigned to them. Although government and contractor staff will often work in a coordinated environment, their areas of responsibility will be separate. However, contractors shall be responsible for generating trouble tickets and documenting results. In this case, responsibilities and hand-off of responsibilities will be clearly documented in ticket management system.

- 14.1.2. The performance of Government FTEs will not be considered in the evaluation of contractor's performance. Contractor and Government employee work can be easily identified with existing problem management tools. Work assignments are made through the ticket management tool; thus making it easy to track and monitor performance.

- 14.1.3. Currently, contractors and Government FTEs effectively coordinate their responsibilities on operational teams. It is expected that this approach will work well in the future. GSA will share all relevant information about Government FTE who will coordinate with contractor resources during Phase-In.

#### **15. STANDARDIZED ENTERPRISE RESOURCE MANAGEMENT (ERM) FRAMEWORK**

- 15.1. The Contractor shall use, as part of its technical support services, a standardized enterprise resource management (ERM) framework to manage the infrastructure. The Contractor may use GFE and supplement licenses to ensure deployment throughout the infrastructure or utilize a standard ERM framework comprising solutions from one or more vendors. This standardized ERM framework may consist of a single- or multi-vendor solution or a customized suite of point solutions.

- 15.2. The Contractor shall support the legacy product sets while assisting GSA in its transition to a standardized ERM framework. Because the legacy product sets involve all aspects of the task order, the Contractor shall work with GSA to transition to a standardized ERM framework.

- 15.3.** The standardized ERM framework may support functionality of software designed specifically to support a piece of hardware or other software. For example, a hardware configuration application or a data backup and restore solution.
- 15.4.** The framework shall perform the following functions:
- 15.4.1. Asset Management – The standardized ERM framework shall serve as the configuration management database for information about all assets.
  - 15.4.2. Ticket Processing – The standardized ERM framework shall maintain, assign and track incidents, requests and complaints. The standardized ERM framework shall be capable of linking related or recurring incidents, requests and/or complaints.
  - 15.4.3. Remote Control – The standardized ERM framework shall enable technical support staff to remotely control a workstation for the purpose of diagnosing and repairing incidents and providing assistance to customers.
  - 15.4.4. Automated Software Deployment – The standardized ERM framework shall facilitate automated deployment of new software, software upgrades, patches, hot fixes, etc. Automated deployment must provide the capability to create installation packages which can be copied to, and distributed via CD/DVD, and loaded on PCs without requiring network connectivity
  - 15.4.5. Report Generation – The standardized ERM framework shall support recurring and one-time reports (dashboard and detailed) by and of, at a minimum, organizations, customers, assets, type of support requirement, responses to support requirements and performance measurement data. The government shall have access to the framework to produce reports.
  - 15.4.6. Self Help – The standardized ERM framework shall empower customers to find answers to their questions about the information technology infrastructure. The knowledgebase shall house applicable standards, policies, guidelines and procedures. It shall include details about ongoing service outages, planned outages, the software release schedule and other relevant issues. It shall also support searching solutions to common problems. The system, available via telephone and web interface, shall result in fewer incidents reported to the help desk. There shall be a reporting capability to independently verify its effectiveness as a self-help tool
  - 15.4.7. Delegation – The standardized ERM framework shall support access by other personnel including those in business lines and other programs to support their requirements. Delegation may include additional customization of features in the standardized ERM framework. The Contractor shall segment data so that users, to whom the standardized ERM framework is delegated, have access to the data for their business line or program.
  - 15.4.8. Other Features – The standardized ERM framework may interface with other applications and services to offer additional features or more timely

response (e.g. an automated call distribution (ACD) or interactive voice response (IVR) capabilities).

- 15.4.9. Availability - The Contractor shall ensure that the standardized ERM framework has an availability of 99.9%.

## 16. ACCESS TO THE STANDARDIZED ERM FRAMEWORK

The Government requires access rights to any data/systems in the standardized ERM framework in use on this task order so the Government may perform the following tasks:

- 16.1. Monitor contractor performance.
- 16.2. Monitor status of open/closed tickets.
- 16.3. Enter data for work performed.
- 16.4. Generate reports.
- 16.5. Other uses determined by the Government.

Approximately 200 Government employees will require access to the standardized ERM framework.

## 17. TASK ORDER MANAGEMENT

- 17.1. **Kick-off Meeting.** At Government discretion, a task order kickoff meeting may be held at a Government location to be determined. The purpose of the meeting shall be to introduce key personnel from the Contractor and the Government, review and develop a Phase-in baseline Program Management Plan (PMP), identify task order ground rules, and review requirements and expectations. The Contractor shall prepare a kickoff meeting report capturing all topics discussed at the meeting.
- 17.2. **Phase-In.** The Contractor shall perform in accordance with the accepted Phase-in plan. The Contractor will acquire a full understanding of GSA business activities, application systems, IT infrastructure, and present GSA and contractor staff resources. A detailed Phase-in plan is a deliverable of this task order. Site access will be permitted during phase-in to the extent it does not interfere with the operation of the incumbent contractor. The Contractor shall coordinate with the COTR for site access permission.
- 17.3. **Phase-Out.** The Contractor shall maintain full task order compliance during the period of time leading up to task order expiration or termination. The Contractor shall submit, to the COTR, a phase-out plan as a deliverable of this task order. The Contractor shall develop the plan within 60 days of task order award and shall update the phase out plan during the life of the task order. The phase-out plan shall be provided to the Government upon request and shall include:
  - 17.3.1. At the end of the period of performance, the Contractor shall assist with transitioning to a new contract/task order. (Note that the transition may be to a Government entity or to another contractor) The Contractor shall assist the Government in planning and implementing a complete transition from this task order to the incoming support provider. This shall include formal coordination with the Government and incoming provider staff, and

management and delivery of soft copies of existing policies, procedures, documentation, hardware, software, and required metrics and statistics.

**17.4. Personnel.** The Contractor shall designate an individual to serve as the main point of contact for technical issues and serve as the supervisor or task order manager for personnel performing work under each task. This individual shall serve as the main point of contact with GSA COTR(s) for technical issues and day-to-day task order management.

17.4.1. Task order management shall allow for staffing flexibility, resulting in nimble, efficient, cost-effective response to short notice increases and decreases in requirements. Changes in staffing may result from unforeseen events (e.g. major relocations, emergency situations, disaster relief, executive mandates, organizational changes, COOP) or technical enhancements (e.g. data center management, new products, security related upgrades, service level fluctuations) or special projects such as support of the PTT (Presidential Transition Team).

## **18. TASK ORDER RESPONSIBILITIES COMMON TO ALL SUB-TASKS**

The Contractor shall designate personnel to perform the following work in support of activities associated with the provisioning and day-to-day management of the information infrastructure environment specified in each sub-task order:

**18.1. COOP Support.** The Contractor shall architect IT infrastructure at the COOP site(s); coordinate with GSA OCIO teams and local Telco for installation of multiple, highly redundant communications links as appropriate; manage IT equipment at COOP sites and designated telework GFE; participate in COOP exercises; engineer data redundancy systems to ensure that critical files are available in accordance with relevant COOP plans; perform desk side and formal training sessions to users and managers on using COOP technology; and coordinate and assist activities in support of disaster preparedness and responses. Activities include, but are not limited to, preparing and maintaining rosters of affected persons and other documentation, participating in meetings and event activities, and researching and evaluating technology to improve agency preparedness including:

18.1.1. COOP documentation creation and maintenance.

18.1.2. Configuration and implementation of COOP HW/SW replacement/upgrades.

18.1.3. Participation in COOP exercises and other related events.

**18.2. Configuration Control and Technical Support.** The Contractor shall perform the following tasks associated with the day-to-day management of the sub-tasks:

18.2.1. Implement all modifications, enhancements, and problem corrections authorized by GSA management.

18.2.2. Develop and maintain system documentation including diagrams.

18.2.3. Recommend actions to improve productivity and strengthen configuration control.

- 18.2.4. Coordinate and assist with certification and accreditation activities required under GSA policies and Government regulations.
- 18.2.5. Coordinate and assist with activities in support of managing assets.
- 18.2.6. Coordinate and assist with activities in support of managing agency-wide licenses.
- 18.2.7. Participate in hardware/software evaluations, and prepare and evaluate cost estimates.
- 18.2.8. Perform security related tasks including scans.
- 18.2.9. The Contractor is required to store data in the standardized ERM framework for each activity, minor and major.

**18.3. Sub-Task Administration.** The Contractor shall perform the following tasks associated with the day-to-day management of each sub-task order:

- 18.3.1. Provide management and technical guidance to contractor employees.
- 18.3.2. Ensure all documentation is completed in accordance with the sub-task requirements.
- 18.3.3. Prepare staffing projections for infrastructure reorganization and improvements.
- 18.3.4. Ensure that the sub-task is staffed, in a timely manner, with adequate personnel in accordance with the sub-task requirements.
- 18.3.5. Monitoring and controlling task and sub-task costs, schedules, and deliverables.
- 18.3.6. Ensure compliance with all applicable policies, directives and regulations.
- 18.3.7. Maintain and update logical and physical diagrams.
- 18.3.8. Work collaboratively with other contractors, Government agencies, and GSA staff participating in this effort to ensure project success.
- 18.3.9. Prepare and deliver Meeting and Review Minutes for all meetings and reviews that the Government requires the contractor's attendance.
- 18.3.10. Assist with business case preparation.
- 18.3.11. Prepare and deliver Meeting and Review Minutes for all contractor/Government meetings and reviews.

**18.4. Operations and Administration.** Operations for peripherals, handheld devices, centralized desktops, laptop computers and remote workstations includes:

- 18.4.1. Submit project plans for modifications/enhancements assigned by the GSA COR, or their designee.
- 18.4.2. Gain GSA management approval of project plan prior to starting maintenance/enhancement.

- 18.4.3. Interface with regional systems coordinators and users to explain system functionality and capabilities.
- 18.4.4. Attend meetings to determine status of various system changes and enhancements, and to discuss upcoming events and other topics.
- 18.4.5. Test all changes/enhancements prior to implementation.
- 18.4.6. Recommend actions to improve desktop productivity, quality, security, and customer satisfaction.
- 18.4.7. Provide controls, access, and management services for local input and output resources, e.g., scanners, printers, files, etc.
- 18.4.8. Manage user, group, and computer accounts.
- 18.4.9. Provide usage accountability, i.e., “charge-back,” to users of resources and services, as defined by GSA.

**18.5. Problem Detection and Correction.** The Contractor shall perform the following tasks associated with the day-to-day management of each sub-task:

- 18.5.1. Track problems with the standardized ERM framework for ticket tracking, problem resolution and reporting.
- 18.5.2. Analyze and resolve problems that arise and/or are assigned by the COTR.
- 18.5.3. Follow GSA policy and procedures regarding problem logging, status updates, and corrections.
- 18.5.4. Identify and analyze problems that indicate systemic issues and recommend solutions to the COTR.
- 18.5.5. Monitor and report on any unusual incidents that could impact performance, safety, or security of GSA operations or personnel.
- 18.5.6. Contact manufacturers for system failures, troubleshooting and coordinate warranty work.

**18.6. ITIL Framework.** The Contractor along with the Government will adopt the Information Technology Infrastructure Library framework over the period of performance of this task order. The Government expects at a minimum the following ITIL processes:

- 18.6.1. Incident Management – The goal of incident management is to maximize infrastructure availability by restoring normal operations as soon as possible with minimum disruption to the business.
- 18.6.2. Problem Management – The goal of problem management is to proactively prevent the recurrence of incidents and problems caused by errors in the infrastructure thereby minimizing the impact on the business.
- 18.6.3. Change Management – The goal of change management is to ensure use of consistent methods and procedures resulting in effective and efficient handling of all changes to minimize impact of incidents upon service.

- 18.6.4. Release Management – The goal of release management is to ensure that aspects of a release are coordinated to include planning, develop\designing, building, testing, approving, communicating, training, deploying, and management of a change release as a single entity.
- 18.6.5. Service Asset and Configuration Management –The goal of service asset and configuration management is to provide a logical model with relationships of the IT infrastructure by identifying, controlling, protecting, verifying, and maintaining accurate information and versions of all assets and configuration items.

**18.7. Conversion to a Performance Based Sub-Task.** If both the Government and the Contractor agree, a sub-task can be converted to a fixed price completion performance based service sub-task after the initial period of performance. The conversion is accomplished as follows. Within ninety calendar days prior to the end of the sub-task initial period of performance, the Contractor shall prepare and submit for Government review, comment, and concurrence:

- 18.7.1. A performance work statement (PWS) that captures all of the types of effort performed during the prior period of performance.
- 18.7.2. A quality assurance plan (QASP). The QASP will address performance standards that relate to the performance requirements, how the contractor’s performance will be measured against the performance standards, and surveillance schedules and methods. The QASP may either be included as part of the PWS or as a separate document.
- 18.7.3. Within sixty calendar days prior to the end of the sub-task initial period of performance, the Government and the Contractor will resolve to their mutual satisfaction any comments or concerns on the PWS and/or QASP. Upon exercise of the option for the first follow-on period of performance, the Government and the Contractor may agree to modify the sub-task to a performance based sub-task.

## **19. COMMUNICATIONS AND DELIVERABLES**

Reports and deliverables shall be submitted in Microsoft Word, Microsoft Excel, Microsoft PowerPoint and/or Microsoft Project and shall be accessible via web. All contractor personnel will be assigned a GSA email account. Email or correspondence shall be provided using the GSA email account. All diagrams shall be delivered in a readable format (PDF or standard formats and hard copy (including oversized diagrams)). All communication to GSA customers is subject to the prior approval of a GSA COR/COTR. Deliverables shall be sorted and rolled up by GSA customer’s location including GSA Service (e.g. FAS, PBS, etc.), GSA Region, City, State and Country. Additional deliverables specific to a sub-task are included in that sub-task.

**19.1. Deliverable #1: Phase-in Plan.** The phase-in plan shall address not less than the following:

- 19.1.1. Manpower requirements
- 19.1.2. Personnel recruitment

- 19.1.3. Personnel orientation
- 19.1.4. Security clearances
- 19.1.5. Site familiarization
- 19.1.6. Comprehensive infrastructure inventory
- 19.1.7. Assumption of responsibility and accountability of GFE
- 19.1.8. Telephone services
- 19.1.9. Contractor provided supplies and equipment
- 19.1.10. Schedule (including milestones)
- 19.1.11. Transition plan
- 19.1.12. COOP

**19.2. Deliverable #2: Phase-Out Plan.** The phase-out plan shall address at a minimum:

- 19.2.1. Procedures for retaining the staffing levels necessary to maintain required task order services through the day of task order expiration or termination.
- 19.2.2. Procedure and responsibilities for performing physical inventory and reconciliation of GFE.
- 19.2.3. Procedure and responsibility for reconciling and certifying material and equipment on-hand levels and accuracy.
- 19.2.4. All costs to the Government, which may occur as a result of transition.

**19.3. Deliverable #3: Project Kickoff Report.** The Contractor shall prepare a kickoff meeting report capturing all topics discussed at the Project Kickoff meeting

**19.4. Deliverable #4: Sub-Task Monthly Reports.** By the 5th working day of each month, or at the frequency noted next to the below sub-items, the Contractor shall submit a Sub-Task Status Report to the GSA PM, COR, and Sub-Task COTR(s), for the previous month through ITSS or mutually agreed upon means. For sub-tasks that have multiple sub-sections, the report needs to categorize the following specifications by sub-section.

- 19.4.1. Key accomplishments and problems encountered for Current Month and FY to date including the performance metrics identified in Attachments 18 and 26 to be reported on a monthly basis.
- 19.4.2. Service level performance -- Plan vs. Actual for Current Month and FY to date.
- 19.4.3. Staffing hours and expenditures -- Plan vs. Actual for Current Month and FY to date.
- 19.4.4. On Call schedule for staff – Identify points of contact and schedule for next month.
- 19.4.5. Team On-site Coverage schedule for next month.
- 19.4.6. Contractor Entrance/Departure Checklist for previous month.

- 19.4.7. NOC Schedule of Staffing Plans including on-call schedule when appropriate for next month.
- 19.4.8. Outage Report – Identify outage occurrences during the previous month and causes, Identify planned outages for next month.
- 19.4.9. Task Order Administration – Status of in-process and completed sub-task modifications.
- 19.4.10. Key Issues Requiring GSA Management Attention.
- 19.4.11. Productivity Accomplishments and Recommendations.
- 19.4.12. Cost Efficiency Accomplishments and Recommendations
- 19.4.13. Adds, Moves and Changes
- 19.4.14. Backup Summary Report. (weekly: Submitted each Monday for previous week)

**19.5. Deliverable #5: Sub-Task Management Plan (STMP).** The Contractor shall develop and deliver a STMP that is based on the Contractor’s proposed solution for the sub-task. The Contractor shall provide STMP Updates on a monthly basis. The Contractor may add additional information to the STMP with approval from the COR. At a minimum this STMP shall include:

- 19.5.1. All technical activities (including documentation development) identified and organized in a Work Breakdown Structure (WBS) at a level of detail sufficient for the Contractor to manage the work at no less than at a week by week basis. The Contractor shall prepare the WBS in Microsoft Project.
- 19.5.2. Action Item Log.
- 19.5.3. A Gantt chart that contains activities and milestones pertinent to the Contractor’s completion of the technical activities.
- 19.5.4. All standards followed in support of these requirements.
- 19.5.5. Description and expected result of each WBS level or milestone in the STMP.
- 19.5.6. An estimate of the duration and level of effort (by labor category) for all elements of the WBS.
- 19.5.7. A matrix of all deliverables, their version/release, and planned delivery dates.
- 19.5.8. A matrix of all personnel assigned to the program and total aggregate level of effort for the task
- 19.5.9. Status of current and planned initiatives and programs.
- 19.5.10. Budget information (planned versus actual, including incurred but not billed, by task) using Cost Accounting.
- 19.5.11. Work Item dependencies and interrelationships.

19.5.12. Project staffing levels, pending security clearances, expected staffing changes.

19.5.13. Contractor organizational structure.

19.5.14. Process management and controls.

19.5.15. Any unique hardware and software utilized by the Contractor.

19.5.16. Outreach process to the GSA users.

**19.6. Deliverable #6: Communications Plan.** In order to ensure a flow of accurate and integrated communications to the GSA employees, the Contractor shall develop and deliver a Communication Plan that at a minimum provides the following information:

19.6.1. Methods of communication.

19.6.2. Timing of communication.

19.6.3. Reasons for communication.

19.6.4. Audience.

19.6.5. Roles and responsibilities.

19.6.6. Key messages.

**19.7. Deliverable #7: Configuration Management Plan.** The Contractor shall provide a Configuration Management Plan that identifies and documents the overall methods and procedures necessary to perform configuration management on all information technology components. This plan will describe all configuration management activities that will be performed during the term of the task order such as:

19.7.1. Identification of configuration items.

19.7.2. Software version control and management.

19.7.3. IP addressing standards and management.

19.7.4. Naming conventions and domain Name System/Dynamic Host Configuration Protocol (DNS/DHCP) assignments.

19.7.5. Standard configuration and descriptors.

19.7.6. Configuration upgrade procedures.

19.7.7. Control and implementation of change.

19.7.8. Recording and reporting implementation status.

19.7.9. Conducting configuration audits.

19.7.10. Review and approval cycles as well as approval authority.

The Configuration Management Plan deliverable is not a Change/Configuration Management plan. The Change Management plan shall be delivered as part of 19.14 Deliverable 14: ITIL Milestones and Implementation Plan.

**19.8. Deliverable #8: Incident Report.** In the event of any occurrence within GSA systems or facilities, which may seriously impact GSA operations or personnel (e.g. network component outage); the Contractor shall issue an incident report to the GSA COTR within 4 hours.

**19.9. Deliverable #9: Earned Value Management System (EVMS) Report.** EVMS reporting may be required under the provisions of ANSI Earned Value Management System (EVMS) Standard ANSI/EIA-748-A-1998 (R2002) for IT development, modernization and enhancement. As such, in the event that work is initiated under EVMS, the Government will utilize information provided in the monthly status report. The Contractor may be required to reformat this information or separate the work specific to the developmental effort to allow the Government to meet its reporting requirement.

**19.10. Deliverable #10: Quality Control Plan (QCP):** This task requires the Contractor to maintain a thorough quality control program with the aim of identifying and correcting deficiencies in the quality of services before performance becomes unacceptable.

19.10.1. As part of the Quality Control Program, the Contractor shall develop a Quality Control Plan (QCP) that describes the Contractor's procedures for monitoring performance. At a minimum, the Quality Control Plan shall include the following:

19.10.1.1. A description of the inspection system to cover all services listed on the Performance Work Statement (PWS). The description shall include specifics as to the areas to be inspected, on both a scheduled and unscheduled basis, and the frequency of these inspections.

19.10.1.2. A description of follow-up procedures to ensure that deficiencies are corrected, and the time frames involved in correcting these deficiencies.

19.10.1.3. A description of the records to be kept to document inspections and corrective or preventive actions taken.

19.10.2. The records of inspections shall be kept and made available to the Government, when requested, throughout the performance period, and for the period after completion, until final settlement of any claims under this task order.

19.10.3. The COR will notify the Contractor, in writing, of deficiencies in the plan and allow 5 working days for a revision to be submitted.

**19.11. Deliverable #11: Productivity Improvement Report:** The Contractor shall provide the government with advice and recommendations in the following areas:

19.11.1. Changing technology needs.

19.11.2. Efficiency improvements and costs savings through improved resource usage and staff reductions.

- 19.11.3. Streamlining of operations.
- 19.11.4. Increasing customer satisfaction.
- 19.11.5. Increasing the efficiency of Government Contractor interface.
- 19.11.6. Staff retention improvements.

**19.12. Deliverable #12: White Papers, Studies, Recommendations and Briefing.** The Contractor shall provide white papers, studies, recommendations and briefings, which address specific information infrastructure issues relevant to each subtask.

**19.13. Deliverable #13: Standard Operating Procedures (SOPs).** The contractor shall develop and/or enhance and deliver SOPs that document standard processes in accordance with applicable government standards based on the contractor's proposed solution across the task order (e.g. coordination of all sub-tasks). The contractor shall provide SOP Updates throughout the task order performance period.

**19.14. Deliverable #14: ITIL Milestones and Implementation Plan.** The Contractor shall provide an ITIL Milestones and Implementation Plan that identifies the activities for implementing and supporting the following processes: Incident Management, Problem Management, Change Management, Release Management, and Service Asset and Configuration Management. The plan shall include implementation milestones and progress for each ITIL process area. This plan will be developed and implemented in a collaborative manner with both government and contractor resources. ITIL implementation milestones shall be periodically reviewed and updates incorporated into the plan. The updated plan shall be delivered on a semi-annual basis or when significant changes occur.

19.14.1. ITIL Milestones and Implementation Plan – Phase 1. The Contractor shall develop, implement, and maintain process assets which are processes, procedures, guidelines, forms, and templates. The plan shall also address the following information (at a minimum):

- 19.14.1.1. Roles and responsibilities of the Contractor and the Government related to the development, approval, implementation, and update of process assets.
- 19.14.1.2. Process milestone schedule – dates for tasks related to the development, implementation, and maintenance of process assets.
- 19.14.1.3. Process reporting standards – the format and frequency of reporting on process assets.
- 19.14.1.4. Process architecture and template development – types of process assets and templates for each.
- 19.14.1.5. Process governance recommendations – recommendations to the Government on a governance structure for oversight and approval of process assets and continued development of the GSA ITIL processes.

19.14.2. ITIL Milestones and Implementation Plan – Phase 2: The Contractor shall identify and support activities which build upon Phase I of the ITIL Milestones and Implementation Plan to include incorporation of plans and schedules for ITIL process integration points, process\technology tool integration, escalation procedures, key performance indicators, lessons learned, and ITIL service improvement plans. This work will be done with government interaction and in a collaborative effort.

**19.15. Deliverable Schedule.** The Contractor shall notify the COR as soon as it becomes apparent to the Contractor that a scheduled delivery will be late. The Contractor shall include in the notification the rationale for late delivery, the expected date for the delivery and the project impact of the late delivery.

PARA	MILESTONE/ DELIVERABLE	PLANNED COMPLETION DATE
17.5	Project Kickoff Meeting	DOA + 5 Working days
19.1	1 Phase-in Plan	DOA + 15 Working days
19.2	2 Phase-out Plan	DOA + 60 Working days
19.2	2 Phase-out Plan	As significant changes to the program occur
19.3	3 Project Kickoff Report	5 working days after Kickoff Meeting
19.4	4 Sub-Task Monthly Status Report	By the 5 <sup>th</sup> working day of the month
19.5	5 Sub-Task Management Plan	By the 5 <sup>th</sup> working day of the month
19.6	6 Communications Plan	DOA + 6 weeks (and updated annually)
19.7	7 Configuration Management Plan	DOA + 8 weeks and quarterly thereafter
19.8	8 Incident Report	Within 4 hours of identification of the incident
19.9	9 Earned Value Management Report	By the 5 <sup>th</sup> working day of the month as required by the COR
19.10	10 Quality Control Plan	15 days after award
19.11	11 Productivity Improvement Report	By the 5 <sup>th</sup> working day of the quarter
19.12	12 White Papers, Studies, Recommendations and Briefing	As issues arise and/or at the Government's request
19.13	13 Standard Operating Procedures	DOA + 6 months (and complete update annually plus incremental changes as necessary)
19.14	14 ITIL Milestones and Implementation Plan	10 working days prior to Option Year 3 and updated semi-annually or when significant changes occur.

## 20. SECTION 508 COMPLIANCE

**20.1.** All Electronic and Information Technology (EIT) services procured through this task must meet the applicable accessibility standards at 36 CFR 1194, unless an agency exception to this requirement exists. 36 CFR 1194 implements Section 508 of the Rehabilitation Act of 1973, as amended, and is viewable at: <http://www.access-board.gov/508.htm>

- 20.2.** GSA has installed a variety of hardware and software to facilitate those users with disabilities in accessing the GSA's information infrastructure. The Contractor shall support all such software and hardware, and make recommendations to the Government regarding improvements to its accessibility inventory.

## **Appendix A: Sub-Task A - Program Management**

### **1. BACKGROUND**

GSA has determined that management of infrastructure operations will be centralized under the Office of the CIO. This effort will consist of organizational changes as well as changes in the way we contract for services. The issuance and management of a single task order will offer GSA opportunities to take advantage of economies of scale and realize cost saving. GSA plans to resolve the complexities and difficulties that are characteristic of implementing, integrating, and securing mission-critical IT solutions.

### **2. OBJECTIVES**

The objectives of the Program Management sub-task are as follows:

- 2.1.** Leverage industry-standard best practices for program management.
- 2.2.** Ensure effective delivery of IT infrastructure services.
- 2.3.** Ensure efficient use of government resources through economies of scale and applicable best practices.
- 2.4.** Ensure minimum performance standards are achieved as specified within the task order.
- 2.5.** Minimize to the greatest extent possible risk to the government.
- 2.6.** Ensure the program management team is responsible for performance of subcontractors and partners.
- 2.7.** Provide effective and timely communication among all internal and external customers within the program.
- 2.8.** Ensure a seamless transition into and out of the task order.
- 2.9.** Maximize continuous process improvement to achieve consistent application of processes to effectively deliver services in accordance with agency policies.
- 2.10.** Measure and maintain an acceptable customer satisfaction per that performance metric.

### **3. SCOPE**

The scope of this sub-task is program management services for infrastructure consolidation and operations. Program management services will be utilized to ensure a smooth transition from existing operations to a consolidated model. The Contractor shall be responsible for technical guidance, issue resolution, project management, and contract support including providing comprehensive account support for the task order and associated sub-tasks.

The Government is interested in remaining current and knowledgeable in the latest industry trends that affect the infrastructure provided to their customers. The scope includes contractor developed Productivity Improvement Reports as well as White Papers, Studies,

and Briefings that provide the latest industry trends and specific information infrastructure issues . The Contractor shall provide suggestions for change to the operation and configuration of the infrastructure environment, as appropriate and as required, that will ensure that GSA remains current, efficient, and effective and so that GSA users continue to receive a high level of quality support.

#### **4. TASK ORDER/SUB-TASK PROGRAM MANAGEMENT TASKS**

The following is a listing of tasks that may be required but is not limited to accomplish the objectives listed in Section 2 above:

- 4.1.** Develop, maintain, update and deliver standard operating procedures as required by the PWS.
- 4.2.** Provide integration of standard operating procedures between all sub-tasks.
- 4.3.** Manage assets across the task order including tracking, reporting and maintaining asset inventory.
- 4.4.** Provide overall management of contractor sub-task management.
- 4.5.** Ensure all documentation is completed in accordance with the requirements of the PWS.
- 4.6.** Prepare staffing projections for infrastructure reorganization and improvements.
- 4.7.** Ensure all sub-tasks are staffed, in a timely manner, with adequate personnel in accordance with the requirements of the PWS.
- 4.8.** Monitor and control by sub-task: costs, schedules, and deliverables in accordance with the requirements of the PWS.
- 4.9.** Maintain documentation of configuration management and change control policies and procedures.
- 4.10.** Provide professional graphical illustrations to depict present, proposed, and recommended solutions associated with evaluations, studies, analyses, etc.
- 4.11.** Develop formal communications, documents, White Papers, and Feasibility Studies.
- 4.12.** Provide recommendations for efficiencies on GSA change management efforts.
- 4.13.** Provide material, logistical and resource support for Executive Management Meetings, which relate to contractor services or performance.
- 4.14.** Provide transition support planning.
- 4.15.** Participate in various governing bodies that perform functions including, but not limited to, standards setting and configuration control.
- 4.16.** Periodically provide data and forecast capacity and systems growth in conjunction with OCIO's capital planning requirements and constraints.
- 4.17.** Work collaboratively with other contractors, Government agencies, and GSA staff participating in this effort to ensure project success.

- 4.18. Prepare and deliver Meeting and Review Minutes for all contractor meetings and reviews with the Government.
- 4.19. Provide business case development support.
- 4.20. Develop and implement a method to measure customer satisfaction.

## 5. SUB-TASK ADMINISTRATION

See General Cross-cutting Section 18 - Task Order Responsibilities Common to all Sub-Tasks.

## 6. DELIVERABLES

The following deliverables are required in addition to the deliverable requirements identified in Section 19 of the General Cross-cutting PWS:

- 6.1. **Deliverable #1: Task Order Status Report.** By the 10th working day of each month, the Contractor shall submit a task order Status Report that summarizes activity and financial status across all sub-tasks for the previous month, to the Deliverables Website (ITSS). The essential elements of the report are:
  - 6.1.1. Key accomplishments and problems encountered for the current month and unresolved issues from previous months.
  - 6.1.2. Service level and performance metrics -- Plan vs. Actual for current month and FY to date.
  - 6.1.3. Staffing and expenditures -- Plan vs. Actual for current month and FY to date.
  - 6.1.4. Percentage of work performed by each contractor, identified by business name.
  - 6.1.5. Contract administration – Status of contracting actions in process.
  - 6.1.6. Key issues requiring GSA management attention.
  - 6.1.7. Productivity recommendations.
  - 6.1.8. Cost efficiency recommendations.
- 6.2. **Deliverable #2: Program Management Plan (PMP).** The Contractor shall develop and deliver a PMP that is based on the Contractor's proposed solution across the task order (e.g. coordination of all sub-tasks). The Contractor shall provide PMP updates throughout the task order performance period. The Contractor may add additional areas to the PMP after appropriate coordination and approval from the Government. At a minimum the PMP shall include:
  - 6.2.1. All technical activities (including documentation development) identified and organized in a Work Breakdown Structure (WBS) at a level of detail sufficient for the Contractor to manage the work at no less than at a week-by-week basis. The Contractor shall prepare the WBS in Microsoft Project.

- 6.2.2. Action Item Log.
  - 6.2.3. A Gantt chart, which contains activities and milestones pertinent to the contractor's completion of the technical activities.
  - 6.2.4. All standards followed in support of these requirements.
  - 6.2.5. Description and expected result of each WBS level or milestone in the Sub-Task Management Plan.
  - 6.2.6. An estimate of the duration and level of effort (by labor category) for all elements of the WBS.
  - 6.2.7. A matrix of all deliverables, their version/release, and planned delivery dates.
  - 6.2.8. A matrix of all personnel assigned to the program and total aggregate level of effort for all sub-tasks.
  - 6.2.9. Status of current and planned initiatives and programs.
  - 6.2.10. Budget information (planned versus actual, including incurred but not billed, by sub-task) using Cost Accounting.
  - 6.2.11. Task dependencies and interrelationships.
  - 6.2.12. Project organization.
  - 6.2.13. Contractor organizational structure.
  - 6.2.14. Process management and controls.
  - 6.2.15. Any unique hardware and software utilized by the contractor.
  - 6.2.16. Outreach process to the GSA users.
  - 6.2.17. Communications Plan to include methods, timing and reasons for communication. It should also address the audience, roles and responsibilities, and purpose for communications.
- 6.3. Deliverable #3: Customer Satisfaction Survey.** The Contractor shall develop, administer and document the results of the customer survey.
- 6.4. Deliverable #4: Asset Inventory Report.** The Contractor shall develop and maintain an asset inventory for the task order.
- 6.5. Deliverable #5: Meeting and Review Minutes.** The Contractor shall deliver minutes of meetings and reviews conducted between the Contractor and the Government.

## 6.6 Deliverable Schedule

PARA	MILESTONE/ DELIVERABLE	PLANNED COMPLETION DATE
6.1	1 Monthly Status Report	By the 10 <sup>th</sup> day of the month
6.2	2 Program Management Plan	DOA + 6 weeks (and updated annually)
6.3	3 Customer Satisfaction Survey	DOA + 3 months and then Annually thereafter
6.4	4 Asset Inventory Report	Quarterly
6.5	5 Meeting and Review Minutes	2 working days after the meeting

## 7. PLACE OF PERFORMANCE.

The place of performance for this sub-task shall be government offices at GSA, 1800 F. Street, Washington, D.C.

## **Appendix B: Sub-Task B - Client Management Services**

### **1. BACKGROUND**

- 1.1.** As a result of recent organizational changes within GSA, the GSA OCIO has been tasked with the responsibility of consolidating IT Infrastructure services. Key among these newly consolidated IT infrastructure services is enterprise-wide client and server management. GSA OCIO requires support to enable the Agency to meet its mission goals in a more cost-effective and efficient manner. To achieve this goal, GSA seeks to consolidate contracted support of all such services and embrace a “shared services” model.
- 1.2.** This sub-task provides for agency-wide server and thin client services, electronic messaging, collaborative services, and agency-wide directory services and authentication infrastructure. This includes electronic mail (client and web mail), anti-virus, anti-spam and related messaging security applications, collaborative and groupware applications supporting shared workspace environments, Blackberry support, and web-conferencing. In addition, the Contractor is responsible for the management, integration, propagation and enhancement of directory services. Directory services management includes such disciplines as identity management, provisioning management (workflow and access privileges of user credentials), design, development, and deployment of authentication and directory services solutions. Special projects such as technical support of the Presidential Transition Team, hereafter referred to as the PTT, large scale conference support and large scale move, adds and changes. Conference support and moves, adds and changes are referenced below in section 6.2.4.3 CONFERENCE SUPPORT AND LARGE SCALE MOVES, ADDS, AND CHANGES (MACS) of this PWS.
- 1.3.** This sub-task also provides for desktop services and associated peripheral services. These desktop services include software delivery, automated application deployment, distribution of standard and custom applications, development of desktop guidelines, policies and standards, life cycle planning (refresh cycles, client image development, deployment procedures), integration of applications and peripheral devices, planning, coordination and implementation of large scale client deployments/refreshes, issuance of security policies, and SME support.
- 1.4.** The Presidential Transition Act of 1963 (as amended) authorizes the Administrator of the General Services Administration to provide for the transition of Office of the President of the United States. Preparation for the Presidential Transition begins at the start of each presidential election year. There are many facets to this exercise but in general terms, the GSA OCIO is responsible for ensuring an IT infrastructure is in place and ready to host 500 to 700 workers the day after Election Day. In the past this has involved the wiring of buildings, setup of workstations and design and deployment of the following self contained environments:

- 1.4.1. Data / Voice Communications facilities
- 1.4.2. Email
- 1.4.3. Collaboration
- 1.4.4. Application servers
- 1.4.5. Call Center
- 1.4.6. Intranet site
- 1.4.7. Internet site
- 1.4.8. Workstations
- 1.4.9. Laptops
- 1.4.10. Network printers
- 1.4.11. Scanners
- 1.4.12. Fax Machines
- 1.4.13. Helpdesk Services
- 1.4.14. Ultra-Secure network (serving up to 25 users) within the main network

## **2. OBJECTIVE**

- 2.1.** GSA wishes to implement an IT infrastructure that is consistent with industry best practices and expects the contractor to provide a comprehensive, best value solution for contracted services.
- 2.2.** The objective of this sub-task is to provide technical support services in the areas of client services to include electronic messaging administration and client support, groupware administration and support, directory services administration, small scale and large scale computer deployments, image management, desktop management, and SME support for the General Services Administration. This support will be used to deploy new systems and operate and maintain existing GSA client services. The desktop infrastructure consists of laptops, desktops, docking stations, PDAs, peripheral devices, enterprise management components, management and reporting systems, and associated software.
- 2.3.** The Contractor shall store data in the standardized ERM framework for each activity, minor and major. The Contractor shall coordinate all activities, and shall generate routine and/or ad hoc reports online that aggregate data about activities

## **3. SCOPE.**

The Contractor shall provide the services enumerated in this sub-task to all users of the GSA enterprise infrastructure. The scope of each major component of this sub-task is addressed in their respective sections.

#### **4. EFFORT ESTIMATE**

The basis of the effort estimate to fulfill the requirements described for each major component of this sub-task, with the exception of the PTT, is the total user population of approximately 15,000. The PTT user population varies between 500 and 700.

#### **5. COLLABORATION**

##### **5.1. Client/Remote Mail**

###### **5.1.1. Background and Technical Environment**

5.1.1.1. GSA OCIO provides technical and operational support services for GSA's Enterprise Messaging Services (GEMS). The services consist of system installation, configuration, administration, maintenance, upgrade, enhancement, monitoring, and operation of GSA's electronic messaging environment. This includes all support for internal and internet messaging, mailing lists, e-mail firewalls, reverse-proxy, and anti-spam solutions.

5.1.1.2. GSA currently uses IBM Lotus N/D 6.5.5 for the enterprise messaging infrastructure. GSA's electronic messaging infrastructure is referred to as the "GSA Enterprise Messaging Services" or (GEMS). GEMS consists of a nationwide network of centrally administered and managed, but geographically dispersed, electronic mail servers, messaging gateways, and e-mail firewalls. Fault tolerant servers are located in each region and at most sites where GSA has a major point of presence. GSA's enterprise messaging services has been implemented based on a client-server architecture utilizing the IBM Lotus Domino server and Notes client software. Mail servers have been deployed in Domino clusters of two (2) servers per cluster. A single cluster is currently deployed to each of GSA's 11 regional and four (4) field office locations (identified below). There are two exceptions to the number of clusters deployed above. The two locations in Washington, DC (National Capital Region Building and Central Office Building) each have two (2) clusters deployed. All clusters are configured as active-active using Domino clustering. There is also a single cluster deployed and supported at the EAC facility in Washington, DC.

5.1.1.3. GSA provides users with multiple methods of access to email, calendaring, and contacts functionality: (1) the Lotus Notes client, from within the GSA network, (2) via a Web browser

from within the GSA network or from the Internet via a proxy server, (3) via a remote access server (RAS) dial-up account using Lotus Notes, a Web browser, or Citrix; (4) via a virtual private network (VPN) connection using Notes; and (5) via BlackBerry wireless service. The GEMS internal mail, SMTP gateway, anti-spam server, reverses proxy, and e-mail firewall server hardware requirements consist of the following:

- 5.1.1.3.1. HP DL580 G1, HP DL580 G2, HP DL580 G3, HP DL380 G3 servers
- 5.1.1.3.2. HP MSL5026DLX2, HP MSL5026SL, and HP TL890DLX tape libraries
- 5.1.1.3.3. CISCO 2950 and 6500 series switches
- 5.1.1.3.4. Operating Systems: Microsoft Windows 2000 Server, Microsoft Windows 2000 Advanced Server, Microsoft Windows 2003 Server, Red Hat Linux Enterprise Server 4, Microsoft Windows XP
- 5.1.1.3.5. Mail/SMTP Server: IBM Lotus Domino 6.5.5/7.0.x
- 5.1.1.3.6. Mail Client: IBM Lotus Notes 6.0.x/6.5.5/7.0.x
- 5.1.1.3.7. Anti-Spam: Cloudmark Authority 2.x, Cloudmark Immunity 1.x
- 5.1.1.3.8. E-Mail Firewall: Tumbleweed E-Mail Firewall 6.x
- 5.1.1.3.9. Reverse Proxy: Websphere 4.x
- 5.1.1.3.10. Database: Microsoft SQL Server 2000 Standard Edition, MySQL Standard 4.x
- 5.1.1.3.11. Server Utilities: Sherpa Software Mail Attender, Executive Software Diskeeper 9.x/10.x, McAfee VirusScan 8.x, McAfee GroupShield, McAfee Linux Shield
- 5.1.1.3.12. Backup Software: CA BrightStor ArcServ Backup software
- 5.1.1.3.13. Remote Access/Control: CA Unicenter Remote Control, Windows Remote Desktop, and Windows Terminal Services
- 5.1.1.3.14. Client Utilities: Infocation Mail Archiver, RPR Systems Antrid

## 5.1.2. Objectives

- 5.1.2.1. To maintain and enhance the current GSA Client and Remote mail services, while remaining flexible enough to augment the current environment and explore other available tools sets to provide a consistent, efficient and reliable email infrastructure to include standardized robust archiving capability. GSA is interested in pursuing a greater degree of fault tolerance and disaster preparedness for its electronic messaging system.
- 5.1.2.2. In addition to this, GSA is very interested in achieving a higher degree of standardization across it's enterprise in terms of client side software configuration, archiving, resource scheduling and other configurations which will allow for a uniform user experience.
- 5.1.2.3. GSA has recently concluded an in-depth study of its electronic messaging environment. The results of this study dictate GSA embrace migrating away from the current distributed model toward a consolidation of physical resources and further centralization of administration. GSA intends to accomplish this using Lotus Notes.

## 5.1.3. Scope

- 5.1.3.1. GSA requires 24x7 technical support services for its electronic messaging infrastructure. In addition since this system is one which needs to evolve to respond to the GSA associates' evolving work environment, the includes the development of recommendations for GEMS' improvement including the implementations, configurations, operations, products, and technologies pertaining to those improvements. Therefore, the research, investigation and work associated with the development of those recommendations are part of the scope.
- 5.1.3.2. Systems are physically located at GSA headquarters and 11 regional office buildings, and four (4) field office locations. Headquarters and the regional offices located are in Washington, DC; Boston, MA; New York, NY; Philadelphia, PA; Atlanta, GA; Chicago, IL; Kansas City, MO; Fort Worth, TX; Denver, CO; San Francisco, CA, and Auburn, WA and field offices in Arlington, VA; Vienna, VA; Anchorage, AK; Honolulu, HI, Europe and Asia. In addition to these primary locations, most GSA regions currently operate their own Domino servers, which host regionally developed applications.

## 5.1.4. Requirements.

- 5.1.4.1. The Contractor shall provide GSA with 24x7 technical support services for its electronic messaging infrastructure. GSA requires technical support with troubleshooting and problem solving to identify and resolve problems or issues associated with GSA's electronic messaging environment.
- 5.1.4.2. Specific requirements for GSA's Messaging Infrastructure environment include but may not be limited to:
- 5.1.4.3. GEMS Server Applications Operations and Support
  - 5.1.4.3.1. Monitoring and Maintenance Support
    - 5.1.4.3.1.1. Application Monitoring
    - 5.1.4.3.1.2. Application Software Maintenance
  - 5.1.4.3.2. Software Configuration, Testing, and Deployment Support
    - 5.1.4.3.2.1. Software Configuration
    - 5.1.4.3.2.2. Software Testing
    - 5.1.4.3.2.3. Server Software Deployment and Installation
  - 5.1.4.3.3. Software Configuration Management Support
  - 5.1.4.3.4. Maintain Software Inventory
  - 5.1.4.3.5. Maintain Systems Diagrams
  - 5.1.4.3.6. Scheduled Outage Support
- 5.1.4.4. E-Mail Operations and Support
  - 5.1.4.4.1. Mail Files and Mail-in Database Administration and Maintenance
    - 5.1.4.4.1.1. Mail File and Mail-in Database Creation
    - 5.1.4.4.1.2. Mail File and Mail-in Database Troubleshooting and Problem Resolution
    - 5.1.4.4.1.3. Mail File and Mail-in Database Relocations
    - 5.1.4.4.1.4. Mail File and Mail-in Database Restorations
    - 5.1.4.4.1.5. Mail File and Message

## Purge/Maintenance

- 5.1.4.4.2. Mail List Administration and Maintenance
  - 5.1.4.4.2.1. Mail List Creation and Maintenance
  - 5.1.4.4.2.2. Mail List Troubleshooting and Problem Resolution
  - 5.1.4.4.2.3. Message Distribution to Specified Mailing Lists
- 5.1.4.4.3. Server-side Electronic Messaging Administration, Troubleshooting, and Maintenance
  - 5.1.4.4.3.1. Administration
  - 5.1.4.4.3.2. Troubleshooting and Problem Resolution
  - 5.1.4.4.3.3. Mail Template and Server Utility Deployment
  - 5.1.4.4.3.4. Configuration, Testing, and Upgrades/Updates
- 5.1.4.4.4. E-Mail Client and User Support (Local and Regional Support Staff)
  - 5.1.4.4.4.1. Message Problem Resolution and Support
  - 5.1.4.4.4.2. Mail Client Configuration Assistance and Support
  - 5.1.4.4.4.3. Troubleshooting and Problem Resolution
  - 5.1.4.4.4.4. Mail Archive Support
- 5.1.4.5. Internet Mail Operations and Support
  - 5.1.4.5.1. Server-side Internet Mail Administration, Configuration, and Operations Support
    - 5.1.4.5.1.1. SMTP Mail Gateway Administration
    - 5.1.4.5.1.2. E-Mail Firewall Administration
  - 5.1.4.5.2. Anti-Spam Administration, Configuration, and Operations Support
  - 5.1.4.5.3. Reverse Proxy Administration, Configuration, and Operations Support

- 5.1.4.5.4. E-Mail Monitoring Troubleshooting, and Maintenance
- 5.1.4.5.5. E-Mail Queue and Log Monitoring and Maintenance
  - 5.1.4.5.5.1. Troubleshooting and Problem Resolution
  - 5.1.4.5.5.2. Tracking, Reporting, and Research
- 5.1.4.6. Capacity Planning, Evaluation, Testing, Configuration, and Implementation Support
  - 5.1.4.6.1. Continuously Monitor and Evaluate Infrastructure Systems Performance
  - 5.1.4.6.2. Identify and Report Potential Performance Issues
  - 5.1.4.6.3. Maintain Current Knowledge of Latest Technologies/Capabilities
  - 5.1.4.6.4. Test and Evaluate New Technologies/Capabilities as Requested
  - 5.1.4.6.5. Develop, Test, and Document New Configurations for Deployment and Implementation
- 5.1.4.7. COOP Support
  - 5.1.4.7.1. COOP documentation creation and maintenance
  - 5.1.4.7.2. Configuration and implementation of GEMS COOP Server Software replacement/upgrades
  - 5.1.4.7.3. Participation in COOP exercises and other related events

**Table 2.1.4.1 REQUIREMENTS MATRIX**

<b>CLIENT / REMOTE MAIL</b>	<b>Government</b>	<b>Contractor</b>
<b>Operations and Administration</b>		
Support electronic messaging infrastructure 24x7		X
Provide on-call support outside of core hours		X
Project Management Support	X	X
Provide Software Maintenance Support (non-procurement)		X
Project Plan Management		X
<b>Standard Operating Procedures Development and Maintenance</b>		
Define Client/Remote Mail capability and requirements	X	X
Define services and standards for Client/Remote Mail	X	

<b>CLIENT / REMOTE MAIL</b>	<b>Government</b>	<b>Contractor</b>
Identify possible product enhancement opportunities for improved performance and potential cost savings	X	X
Provide mail file certifications / credentials		X
Provide SME support for client/remote mail tools		X
<b>Configuration Management/Change Control</b>		
Define configuration management & change control policies and procedures	X	
Perform configuration management & change control activities throughout life cycle of support services		X
Document Policies, Procedures, change requests and activities		X
Approve change control results	X	
<b>Training Activities</b>		
Establish training plans and procedures	X	
Provide advanced training, as agreed, to GSA technical personnel to facilitate full exploitation of all relevant functional features		X
Provide training for GSA personnel to improve “how-to-use” skills related to IT service area systems and applications		X
Provide distributed computing support for classrooms, labs and electronic learning events		X
<b>Monitoring and Reporting</b>		
Approve and document service levels and reporting cycles	X	
Measure and analyze performance relative to requirements	X	X
Develop improvement plans where appropriate	X	X
Implement improvement plans		X
Report on service level performance results		X
<b>Chargeback</b>		
Assign user account codes		X
Maintain table for GSA account codes		X
Track utilization		X
Produce cost center invoices		X
Send invoices		X
Respond to GSA inquires		X

## 5.2. Groupware

### 5.2.1. Background And Technical Environment

- 5.2.1.1. The GSA OCIO provides technical and operational support services for GSA’s groupware application and collaboration infrastructure known as GNNI (GSA National Notes Infrastructure). These services consist of system installation, configuration, administration, maintenance, upgrade,

enhancement, monitoring, and operation of GSA's groupware and collaboration environment. In addition, application rollout, replication, directory and server technical support services are provided to organizations maintaining organization specific groupware and collaboration servers throughout the agency. The GSA Central Office Infrastructure Systems Operations Center (ISOC) Facility serves as the central administration and management location for system monitoring and Central Office support.

- 5.2.1.2. There is also a government-owned and operated off-site location with redundant hardware/software that can be put into service in the event of extended downtime of multiple sites or locations. Test, staging and evaluation environments are also maintained and utilized by the team constantly in support of the infrastructure environment.
- 5.2.1.3. GSA currently uses IBM Lotus Notes/Domino collaboration suite. This tool set includes Sametime (Instant Messenger), Quickplace (Virtual Meetings) and Websphere (application environment). GNNI consists of a nationwide network of centrally administered and managed, but geographically dispersed, GSA provides users with multiple methods of access to GNNI: (1) the Notes client, from on the GSA network, (2) via a remote access server (RAS) dial-up account using Notes, a Web browser, or Citrix; and (3) via a virtual private network (VPN) connection using Notes.
- 5.2.1.4. GNNI's implementation is based on a hub and spoke topology using IBM Lotus Domino servers and Notes clients. The primary components of GNNI are the registration server, hub server, and spoke servers. The GNNI hub and registration servers are located in GSA's Central Office location. A single GNNI application spoke server is deployed at Central Office and each of its 11 Regional Office locations. The GNNI registration server connects directly to the GNNI hub server. This server is also located in Central Office. The registration server's purpose is for the registration and maintenance of the Domino Directory and all of its associated certificates and documents. The Domino Directory, which within GSA is referred to as the GSA Address Book, provides all server-related information, certificates, and application-related groups, as well as e-mail specific information related to individuals and mailing lists. The GNNI hub and spoke application servers utilizes replication technology across its topology for updating

the GSA Address Book across the infrastructure and for hosting and replicating all of GSA's national and regional groupware applications' data and designs.

5.2.1.5. The GNNI application and collaboration server hardware consist of the following:

5.2.1.5.1. HP DL380 G3, HP DL 580 G1 and Dell PowerEdge 2850 servers

5.2.1.5.2. HP SSL 1016 SDLT tape libraries

5.2.1.6. The GNNI application and collaboration server and related software consist of the following:

5.2.1.6.1. Operating Systems: Microsoft Windows 2000 Server, Microsoft Windows 2003 Server, Microsoft Windows XP

5.2.1.6.2. Application Server: IBM Lotus Domino 6.5.5/7.0.x, Quickplace 3.x and above, Sametime 3.x and above, Blackberry Enterprise Server 2.2 and above

5.2.1.6.3. Client: IBM Lotus Notes 6.0.x/6.5.5/7.0.x, Blackberry client

5.2.1.6.4. Server Utilities: Executive Software Diskeeper 9.x/10.x, McAfee VirusScan 8.x, McAfee GroupShield

5.2.1.6.5. Backup Software: CA BrightStor ArcServ Backup software

5.2.1.6.6. Remote Access/Control: CA Unicenter Remote Control, Windows Remote Desktop, and Windows Terminal Services

## 5.2.2. Objectives

5.2.2.1. To maintain and enhance the current GSA groupware services while remaining flexible enough to augment the current environment and explore other available tools sets to provide a consistent, efficient and reliable email infrastructure to include standardized robust archiving capability. GSA is interested in pursuing a greater degree of fault tolerance and disaster preparedness for its electronic messaging system.

5.2.2.2. In addition to this, GSA is very interested in achieving a higher degree of standardization across its enterprise in terms of client side software configuration, archiving, resource

scheduling and other configurations which will allow for a uniform user experience.

5.2.3. Scope

5.2.3.1. GSA requires 24x7 technical support services for its groupware infrastructure. Systems making up this infrastructure are located at GSA headquarters and 11 regional office locations. Headquarters and the regional offices located are in Washington, DC; Boston, MA; New York, NY; Philadelphia, PA; Atlanta, GA; Chicago, IL; Kansas City, MO; Fort Worth, TX; Denver, CO; San Francisco, CA, and Auburn, WA. Some regions have deployed and currently maintain their own Sametime, Quickplace and application servers. The Contractor shall assist the Government in consolidating all such resources and deploying and maintaining an enterprise collaboration solution.

5.2.4. Requirements

5.2.4.1. GSA requires high level contract support with troubleshooting and problem solving to identify and resolve hardware and/or software problems or issues, associated with or specific to, the hardware and software identified below. Research, investigation and reports of recommendations regarding implementations, configurations, operations, products, and technologies pertaining to GNNI's groupware and collaboration environments is also required.

5.2.4.2. Below are the specific requirements for GSA's Groupware Infrastructure environment:

5.2.4.2.1. Project Management Support

5.2.4.2.1.1. Personnel/Staffing Plan

5.2.4.2.1.2. Project Plan Development and Maintenance

5.2.4.2.1.3. Standard Operating Procedures Development and Maintenance

5.2.4.2.1.4. Progress Meetings

5.2.4.2.2. GNNI Application and Collaboration Server Operations and Support

5.2.4.2.2.1. Monitoring and Maintenance Support

5.2.4.2.2.2. Systems Monitoring

- 5.2.4.2.2.3. Systems Software Maintenance
- 5.2.4.2.2.4. Software Configuration, Testing, and Deployment Support
- 5.2.4.2.2.5. Software Configuration
- 5.2.4.2.2.6. Software Testing
- 5.2.4.2.2.7. Software Deployment and Installation
- 5.2.4.2.2.8. Software Configuration Management Support
- 5.2.4.2.2.9. Maintain Software Inventory
- 5.2.4.2.2.10. Maintain Systems Diagrams
- 5.2.4.2.2.11. Scheduled Outage Support
- 5.2.4.2.3. GSA Public Address Book Administration
  - 5.2.4.2.3.1. Notes User ID Creation/Registration
  - 5.2.4.2.3.2. Notes User ID Recertification
  - 5.2.4.2.3.3. Organizational Unit/Certifier Creation
  - 5.2.4.2.3.4. Server ID Creation/Registration
  - 5.2.4.2.3.5. Certificate Maintenance
  - 5.2.4.2.3.6. Server Connection Document Creation/Maintenance
  - 5.2.4.2.3.7. ID Cross-Certification
  - 5.2.4.2.3.8. Group Creation/Maintenance
  - 5.2.4.2.3.9. Mail-In Database Document Creation/Maintenance
  - 5.2.4.2.3.10. Domain Document Creation/Maintenance
  - 5.2.4.2.3.11. Program Document Creation/Maintenance
  - 5.2.4.2.3.12. Setup Profile and Policy Creation/Maintenance
  - 5.2.4.2.3.13. Separations Processing and Terminations Database Maintenance
  - 5.2.4.2.3.14. Mail File Inactivity Reporting and Maintenance

- 5.2.4.2.3.15. Replication Maintenance and Conflict Resolution
- 5.2.4.2.3.16. Resource Creation and Resource Database Maintenance and Support
- 5.2.4.2.3.17. GSA Public Address Book Design Template Upgrades and Maintenance
- 5.2.4.2.4. GNNI Nationwide/Regional Application Support
  - 5.2.4.2.4.1. Application Rollout on GNNI
  - 5.2.4.2.4.2. Application Access/Group Configuration Support
  - 5.2.4.2.4.3. Application/Replication Problem Resolution
  - 5.2.4.2.4.4. Application Server Setup and Configuration Support
  - 5.2.4.2.4.5. Application Server Problem Resolution Support
- 5.2.4.2.5. Collaboration Operations and Support
  - 5.2.4.2.5.1. Collaboration Administration, Configuration, Operations and Support
  - 5.2.4.2.5.2. Collaboration Monitoring Troubleshooting, and Maintenance
  - 5.2.4.2.5.3. Collaboration Client Configuration Support
  - 5.2.4.2.5.4. On-line Meeting and Team Room Support
- 5.2.4.2.6. End-User/Technical Staff Support
  - 5.2.4.2.6.1. General Notes client and/or workstation configuration assistance
  - 5.2.4.2.6.2. Troubleshooting/problem resolution
  - 5.2.4.2.6.3. User instruction/education
  - 5.2.4.2.6.4. Database restores
  - 5.2.4.2.6.5. Internet password support
- 5.2.4.2.7. COOP Support
  - 5.2.4.2.7.1. COOP documentation creation and

maintenance

5.2.4.2.7.2. Configuration and implementation of GNNI COOP Server HW/SW replacement/upgrades

5.2.4.2.7.3. Participation in COOP exercises and other related events

**Table 2.2.4.1 REQUIREMENTS MATRIX**

<b>GROUPWARE</b>	<b>Government</b>	<b>Contractor</b>
<b>Operations and Administration</b>		
Support Groupware Infrastructure 24x7		X
Provide on-call support outside of core hours		X
Project Management Support	X	X
Provide Software Maintenance Support (Non Procurement)		X
Project Plan Management		X
Standard Operating Procedures Development and Maintenance		X
Define Desktop/end user capability and requirements	X	
Define services and standards for desktop/end-user capabilities	X	X
Define standard client configuration criteria for groupware	X	X
Train regional and local staff in proper configuration and deployment practices		X
Identify possible product enhancement opportunities for improved performance and potential cost savings	X	X
Provide groupware file certifications / credentials		X
Provide input processing support for activities such as loading media, receiving batch electronic file transmissions, etc.		X
Develop scripts and macro programs to automate standard GSA processes as appropriate (e.g., upgrading desktop profiles)		X
Provide high level support for groupware tools		X
Configuration Management/Change Control		X
Define configuration management & change control policies and procedures	X	
Document Policies, Procedures, change requests and activities		X
Perform configuration management & change control activities throughout life cycle of support services		X
Approve change control results	X	
<b>Training Activities</b>		
Establish training plans and procedures	X	
Provide advanced training, as agreed, to GSA technical personnel to facilitate full exploitation of all relevant functional features		X

<b>GROUPWARE</b>	<b>Government</b>	<b>Contractor</b>
Provide training for GSA personnel to improve “how-to-use” skills related to IT service area systems and applications		X
Provide distributed computing support for classrooms, labs and electronic learning events		X
<b>Software Management</b>		
Establish software license management policies	X	
Establish supported software portfolio	X	
Document Software License policy and portfolio		X
Negotiate and procure software site or individual licenses that protect GSA right to use the software	X	
Track software assets (user, location, asset id, finances)		X
Maintain software product inventory as needed	X	X
Establish software migration/upgrade standards and policies	X	
Develop detail procedures to ensure low-risk migration/upgrade		X
Test new releases of supported software to ensure conformance with GSA service level requirements		X
Install new releases of supported software on servers & standalone/mobile PCs		X
Initialize desktop devices, as needed, in conjunction with migration/upgrade		X
Verify desktop is fully functional following the migration/upgrade process		X
Provide technical assistance during conversion as requested		X
<b>Groupware Maintenance and Enhancement</b>		
Disconnect, pack and ship the units to new location		X
Unpack, reconnect, test units and attached devices at new location and install them		X
Perform hardware add and change at end user location		X
Perform network based or CD distribution for software change and add		X
<b>Monitoring and Reporting</b>		
Approve and document service levels and reporting cycles	X	
Measure and analyze performance relative to requirements	X	X
Develop improvement plans where appropriate	X	X
Implement improvement plans		X
Report on service level performance results		X
<b>Chargeback</b>		
Assign user account codes		X
Maintain table for GSA account codes		X
Track utilization		X
Produce cost center invoices		X

Send invoices		X
Respond to GSA inquires		X

### 5.3. Directory Management Services

#### 5.3.1. Background

- 5.3.1.1. GSA’s primary Directory Service consists of a nation wide deployment of Active Directory, which provides support to over approximately 15,000 clients. The deployed infrastructure, with over 60 Domain Controllers, supports a customer base, which is distributed across the United States in the eleven regional offices, over 580 field locations and a small presence in Europe and Asia. The Active Directory Forest is an empty root design with a single sub domain supporting GSA resources and credentials. GSA also has a number of other directory services based applications such as its electronic messaging solution (Lotus Notes Domino) and its personnel management system (CHRIS).
- 5.3.1.2. GSA has recently completed a successful pilot aimed at exploiting its established directory services infrastructures to achieve a higher degree of single sign-on (SSO), security and provisioning. The number of users currently being supported with SSO is less then 500 and are primarily located at GSA Headquarters and within various regions. The infrastructure supporting the leveraging of directory services is detailed below.
- 5.3.1.3. Operational support of GSA’s AD deployment is currently carried out under the auspices of FSS but will become the responsibility of GSA OCIO upon award of this PWS.

**TABLE 3.1.1 (BACKGROUND)**

<b>Identity Management Technical Environment / Benefits Matrix</b>			
<b>Solution</b>	<b>Benefit Area</b>	<b>Descriptive Statement</b>	<b>Impact</b>
LDAP Directory Management	Centralized LDAP directory supporting internal/external authentication	Enterprise Active Directory Infrastructure, providing a centralized resource management directory to assist in end-user access to distributed systems. Centralized Policy and security for passwords and system configuration. Supporting a central authentication directory for integrated applications and an external directory providing a central LDAP directory for external end-user authentication.	Reduced support cost by leveraging a standards-based directory for support of GSA end-user management, allowing for shared resources across the different GSA business lines.
Password Management, Self Service portal	Password synchronization with LDAP enabled directories (Lotus and AD) and backend database solutions which include SQL, Sybase, oracle, etc...	Enterprise password management through password synchronization with self service password management available through a web portal.	Reduced password related help desk calls due to self-service password management. Enhanced security with one password utilized by disparate applications and enforcing password complexity rules.
Lotus Notes ID - File Synchronization, Identity Management	Lotus Notes	Password synchronization of the Lotus Notes ID File.	Allows for password synchronization of the lotus notes client logon with Windows password authoritative password store.

Single Sign On, User Interface	Client and web based application	Enterprise single sign-on for multiple and disparate applications using screen scrape technology.	Increased user productivity. Increased security through support of multiple authentication models. Decrease in password related helpdesk calls. Centralized administration of user passwords.
Data Normalization, Identity Management	Meta Base Join engine for work flow development, and Business logic. Provisioning Users, normalizing and synchronizing data.	Provides a centralized repository for the meta verse. Data synchronization across heterogeneous directories and applications databases. Work flow for authoritative user attributes and provisioning. Data redundancy achieved through use of MS SQL database and Microsoft clustering services.	Data redundancy. Centralized data repository leads to decreased cost for application data administration for application owners.
Database utilized by MIIS for data storage, Identity Management	Active Directory, Metadirectory	Provides a backend data storage solution for metadirectory.	Data redundancy through clustering of the databases. Easy integration with MIIS solution

### 5.3.2. Objectives

5.3.2.1. Operational goals for Directory Services include: Password and Directory synchronization, Single Sign-On (SSO) capability, especially with Lotus Notes, improved and centralized user provisioning capabilities, data normalization and standardization of disparate data stores, and electronic authentication for system access and transaction processing.

5.3.2.1.1. Password synchronization and Single Sign-On (SSO):

5.3.2.1.1.1. Users will benefit from a simplified authentication process (fewer passwords are better).

- 5.3.2.1.1.2. Password authentication service for Lotus Notes is critical. Directory user information must synchronize with Lotus Notes.
- 5.3.2.1.1.3. Enable SSO for all web-based applications.
- 5.3.2.1.1.4. Normalize and standardize user information across all data stores.
- 5.3.2.1.2. Directory synchronization:
  - 5.3.2.1.2.1. Ensure the accuracy and consistency of information contained in all directories.
  - 5.3.2.1.2.2. Make user commissioning and decommissioning easier and more secure.
    - i. User ID's must be up-to-date
    - ii. Push ID badge information to wherever it is needed.
  - 5.3.2.1.2.3. Prevent the propagation and distribution of inaccurate information across directories during the migration to AD.
  - 5.3.2.1.2.4. Synchronize data across the enterprise; i.e. - Notes user data will agree with AD and CHRIS (HR System).
  - 5.3.2.1.2.5. Enable enterprise directory management.
- 5.3.2.1.3. E-Authentication services:
  - 5.3.2.1.3.1. Enable identity and authentication services;
  - 5.3.2.1.3.2. Enable web-based Single Sign-On (SSO) for applications,
  - 5.3.2.1.3.3. Enable sharing of data inter-office, inter-service (business line), and inter-agency.
  - 5.3.2.1.3.4. Allow GSA users and outside clients to sign-on with certificates they

already own.

5.3.2.1.4. Support all four levels of Federal Assurance.

5.3.2.1.5. HSPD 12 – Logical integration of FIPS 201 compliant credentials

5.3.2.2. The following are the goals and requirements for the GSA e-Authentication system:

5.3.2.2.1. Enable Enterprise Level User Authentication:

5.3.2.2.1.1. SSO for both internal and external customers

5.3.2.2.1.2. Enable inter-office, inter-service (business line), and inter-agency sharing of data.

5.3.2.2.1.3. Allow GSA users, customers and vendors to use non-government issued credentials from a variety of sources to conduct transactions with the government.

5.3.2.2.2. Support Federal levels of assurance:

5.3.2.2.2.1. Enforce all four levels of authentication assurance, levels I/II/III internally and externally (username, password, or certificate); levels IV will be available when needed.

5.3.2.2.3. Comply with E-Gov Initiative

5.3.2.3. The following are the goals and requirements for the GSA Identity and access management solution.

5.3.2.3.1. Enable Single Sign-On (SSO) capability for all web-based applications and Lotus Notes.

5.3.2.3.2. Ensure accurate and consistent information across all directory stores; enable many non-LDAP aware applications to utilize other directory store information.

5.3.2.3.3. Enable identity and authentication services; sharing of data inter-office, inter-service, and inter-agency; with the critical requirement of allowing GSA users and outside clients to sign-on with Federated Credentials or Federal Bridge approved certificates.

- 5.3.2.3.4. Perceptibly improve GSA overall security processes and risk level for Authentication and access management.
- 5.3.2.3.5. Implement Provisioning and role based management of credentials.
- 5.3.2.4. The following are the goals and requirements for the GSA Single Sign On implementation:
  - 5.3.2.4.1. Enable Single Sign-On (SSO) capability for internal customer to GSA application systems
  - 5.3.2.4.2. Ensure the stored credentials are maintained and secured in the LDAP directory.
  - 5.3.2.4.3. Reduce helpdesk calls for password resets
  - 5.3.2.4.4. Provide GSA end users with a solution to reduce logins and save time.
  - 5.3.2.4.5. Leverage the Identity Management infrastructure, which synchronizes passwords and logins.

### 5.3.3. Scope

- 5.3.3.1. GSA requires the support of its enterprise wide Directory Services assets and related projects which will leverage GSA's investment in these directory based technologies. These projects include E-Authentication, HSPD12, identity and access management and single sign-on.
- 5.3.3.2. While GSA has several directory based applications, core among them is a nation wide deployment of Active Directory which provides support to over approximately 15,000 clients. The infrastructure is deployed with over 60 Domain Controllers supporting a customer base which is distributed across the United States in the eleven regional offices, over 500 field locations and a small presence in Europe and Asia. The Active Directory Forest is an empty root design with a single sub domain supporting GSA resources and credentials. All technical core infrastructure components are leveraged in this design and require support.

### 5.3.4. Requirements

- 5.3.4.1. GSA requires support of the primary tool used for administering the AD environment which is NETIQ security administration suite. This current infrastructure supports a distributed delegation model. GSA requires support as it

transitions from this model to a model capable of supporting a centrally supported environment. The environment will require standard administrative support for day to day management. It will also require SME support for planning, engineering and integration. Active Directory is leveraged to distribute Group Policies for login scripts, security and computer management. This infrastructure requires support of an AD integrated DNS with multiple secondary zones and a WINS environment in support of legacy resources. GSA has migrated 90% of its user and resource population across GSA. Support must continue for the legacy infrastructure while finalizing migration of all users and resource.

- 5.3.4.2. GSA requires contractor support for Directory Management services in order to support the GSA Enterprise implementations for Directory Services (LDAP Systems), E-Authentication, HSPD12 (PIV II specific to Logical Access), Identity and access Management, password management and Single Sign-On. These technologies, supporting credentialing, authentication and access management, are tightly integrated and carry a high level of interdependence. The primary objectives of this sub-task is the development, integration and support a secure and standard deployment approach of GSA's overall Identity and access Management solution(s) and integration with application systems across GSA. Fulfillment of these objectives will result in the minimization of manual provisioning and centralization of password management within the GSA OCIO.
- 5.3.4.3. Identity information about people, applications, and resources is scattered throughout the GSA enterprise network, and is continuing to proliferate. While an increasing amount of this information is being gathered and stored in the Active Directory service, much remains in widely distributed data stores and specialized applications like Lotus Notes that require unique and proprietary access methods.
- 5.3.4.4. E-Authentication: GSA requires support for the GSA e-authentication effort underway. E-Authentication is a part of the Presidential Management Agenda; all Federal agencies are required to implement a solution consistent with the Federated model. The E-Authentication initiative provides specification and standards to enable trust and confidence in online transactions through the establishment of an integrated policy and technical infrastructure for electronic authentication. GSA

requires support in implementing a solution consistent with the Federated Model developed by the E-Authentication Program Management Office. Technical reference material can be found at [www.cio.gov/eauthentication](http://www.cio.gov/eauthentication).

- 5.3.4.5. This solution will be based on the standards to be developed by the Information Technology Architectural Planning Committee (ITAPC) Application Subcommittee and implemented as a centralized Model. This solution requires support integrating a SAML environment with Level 1 and 2 as well as PKI support for level 3 and 4 credential based application systems. The level of assurance required for the GSA application systems has been identified within the ramp up plan issued to OMB. Risk assessments are conducted by the security office to determine the level of assurance. As part of this initiative, GSA requires support implementing its plans to leverage this architecture in support of future enterprise wide Identity and access management solution planning and development efforts.
- 5.3.4.6. HSPD12- (Home Land Security Presidential Directive): GSA requires support for PIV II, which is based on logical access. The Agency further requires support of the infrastructure, which is still in development due to compliance testing with vendor supported components, to support this implementation. Support is required for the basic requirements in support of this initiative which includes technical integration of all components required under HSPD12. The business processes and program policy is supported by the GSA PMO office, and will require assistance from the operational support groups to complete a successful deployment of a FIPS 201 compliant systems. This requirement will ensure standards for integration into the current infrastructure systems and are supported by the Directory Management office, and are in compliance with GSA identity and access management direction.
- 5.3.4.7. Identity and Access Management. GSA requires support for its Identity management system which consists of an integrated solution with the Active Directory and Lotus Notes infrastructure. The primary components of this system requiring support are the Identity Management infrastructure which includes MIIS (Microsoft Identity Integration Server), M-Tech - Psynch for password management/self service portal and M-Tech - IDsynch for supporting password synchronization with the lotus ID File as well as workflow and provisioning. GSA is in the early planning stages of

implementing the overall solution for Identity Management. The primary requirements are to continue to support integration of these technologies into GSA infrastructure and application systems.

- 5.3.4.8. Single Sign On: GSA requires support for the technology used to support a single sign on implementation for the internal GSA user base. This technology leverages Active Identity (secure login), which provides end-users with a screen scrape solution to leverage stored credentials within the LDAP directory for access to GSA application systems. This solution is scripted base allowing for error handling with the different application systems. The requirements for this implementation includes support for current client deployment, testing and planning of upgrades, development of scripts for implementing new GSA applications, and support of current customized scripts developed to support GSA enterprise application systems. The error handling testing requirements will be limited as we move forward with password synchronization and identity management.

**Table 2.3.4.1 REQUIREMENTS MATRIX**

<b>Directory Services Management</b>	<b>GSA</b>	<b>Contractor</b>
<b>Operations and Administration</b>		
Assist the Directory Services Program Management Office (PMO) in defining policies and procedures, and overall program management support		X
Support GSA wide internal and external LDAP Directory Authentication		X
Support the management, administration, and improvements of Directory Services programs and initiatives		X
Support Delegated Administration roles and responsibilities to all support groups in GSA		X
Provide technical development and support for GSA Directory Services standards, which include the GSA Directory Naming Standards, E-Authentication Application integration standards, schema development standards and overall Identity Management Standards support.	X	X
Support Integrated DNS, WINS, DHCP and core functionality of Active Directory		X
Support integration of PKI/SmartCard for logical access to the Directory Management environment		X

<b>Directory Services Management</b>	<b>GSA</b>	<b>Contractor</b>
Support technical implementation of complete enterprise-wide Single Sign-On (SSO) and user data security credentials within GSA systems/applications.		X
Provide technical assistance and support for developing HSPD 12 PIV I/II integration with logical systems		X
Provide continued engineering support, including technical support ensuring security is always prioritized for the enterprise-wide E-Authentication solution.		X
Develop project plans and requirements in support of GSA business application systems required to integrate into the E-Authentication technical solution		X
Provide engineering support for integration of E-Authentication architecture into the enterprise application environment and for any future initiatives		X
Provide project management and integration support for ongoing and future Directory Services and E-Authentication projects, Deployments and initiatives.	X	X
Provide integration support for SAML (security assertion markup language) with GSA application systems identified to move towards E-Authentication.		X
Assist, Manage and provide technical support to services and staff offices with migration efforts to the programs our office develops and supports.		X
E-Authentication architecture - GSA has a working model which is being developed. This model leverages a session Directory for managing and integration of the diverse applications across GSA. This model requires API and LDAP coding support in effort to integrate with authentication schemes leveraged by the diverse application systems managed by the business lines with in GSA.		X
GSA will require that the technical support group can plan, architect, integrate, and develop support models based on Identity and Access Management solutions		X
Support architecture and integration of GSA level 1 and 2 Application systems utilizing SAML (Security Assertion Markup Language) which requires Java development		X
Support integration of PKI requirements for level 3 and 4 application systems		X
Support the meta-directory environment for data normalization and synchronization of disparate directories within GSA.	X	
Provide support for account provisioning with all consolidated data directories/databases with in the Meta environment and future integrated systems		X

<b>Directory Services Management</b>	<b>GSA</b>	<b>Contractor</b>
Provide technical development and support for GSA Directory Services standards, which include the GSA Directory Naming Standards, E-Authentication Application integration standards, schema development standards and overall Identity Management Standards support.	X	X
Support HSPD 12 PIV I/II integration which includes system management and design, automation of business processes defined for identity proofing, integration support of card management for authentication into directory systems for logical and physical access.		X
Develop automated workflow for role-based provisioning supporting GSA infrastructure and application systems.		X
Provide technical guidance and planning for new mandates, regulations or directives issued which apply to the technical focus this office has responsibility for.		X
<b>Configuration Management/Change Control</b>		X
Define configuration management & change control policies and procedures	X	
Document Policies, Procedures, change requests and activities		X
Perform configuration management & change control activities throughout life cycle of support services		X
Approve change control results	X	
<b>Training Activities</b>		
Establish training plans and procedures	X	X
Provide advanced training, as agreed, to GSA technical personnel to facilitate full exploitation of all relevant functional features		X
Provide training for GSA personnel to improve “how-to-use” skills related to IT service area systems and applications		X
Provide distributed computing support for classrooms, labs and electronic learning events		X
<b>Software Management</b>		
Establish software license management policies	X	X
Establish supported software portfolio		X
Negotiate and procure software site or individual licenses that protect GSA right to use the software	X	
Track software assets (user, location, asset id, finances)		X
Maintain software product inventory as needed		X
Establish software migration/upgrade standards and policies		
Develop detail procedures to ensure low-risk migration/upgrade		X
Test new releases of supported software to ensure conformance with GSA service level requirements		X

Install new releases of supported software on servers and standalone/mobile PCs		X
Initialize desktop devices, as needed, in conjunction with migration/upgrade		X
Verify desktop is fully functional following the migration/upgrade process		X
Provide technical assistance during conversion as requested		X
Ensure directory server availability		X
Perform directory software upgrades		X
Perform add, change or delete to individual accounts		X
Maintain directory accuracy across GSA infrastructure		X
Define directory support policies and procedures	X	X
<b>Monitoring and Reporting</b>		
Approve and document service levels and reporting cycles	X	X
Measure and analyze performance relative to requirements		X
Develop improvement plans where appropriate		X
Implement improvement plans		X
Report on service level performance results		X
<b>Chargeback</b>		
Assign user account codes	X	
Maintain table for GSA account codes		X
Track utilization		X
Produce cost center invoices		X
Send invoices		X
Respond to GSA inquires		X

#### 5.4. BlackBerry Technology Support (See Modification AS09)

##### 5.4.1. Background

Currently the BlackBerry servers are located throughout the regional offices and Central Office. There are approximately 4,500 BlackBerry users agency-wide. There are 11 locations with primary BEAS servers with 4 failover locations. These servers are centrally managed. The following information is provided:

- 5.4.1.1. BlackBerry servers – 16
- 5.4.1.2. BlackBerry SQL server – 1
- 5.4.1.3. BlackBerry Backup SQL server – 2
- 5.4.1.4. WIC server (SQL) – 1
- 5.4.1.5. Metamessage server (SQL) - 1

5.4.1.6. BlackBerry Backup servers – 2

5.4.1.7. Lotus Notes servers – 2

5.4.2. Objective

GSA is seeking full enterprise-wide technical operational support for its existing BlackBerry infrastructure.

5.4.3. Scope

The Contractor shall provide constant vigilance on emerging technology and provide recommendations on the proper application of such technology to the GSA environment. Evaluate and implement new wireless technology in support of GSA nationwide, including GSA BlackBerry Infrastructure.

5.4.4. Requirements

**Table 4.7 – 1 BlackBerry Services Typical Work Item Examples**

<b>BlackBerry Technology Support</b>	<b>Government</b>	<b>Contractor</b>
<b>Operations and Administration</b>		
Provide appropriate analysis and recommendations regarding GSA’s BlackBerry Enterprise Infrastructure.	X	X
Provide support to resolve BlackBerry support problems and other day-to-day technology issues as requested by the Government to include server and technical systems support of the BlackBerry Infrastructure.	X	X
Provide support and input to system audits by developing corrective actions to such audits.		X
Evaluate and implement new wireless technology in support of GSA nationwide, including GSA BlackBerry Infrastructure.		X
Provide technical recommendations regarding the purchase of new equipment, system configuration, equipment operations, data storage, and software applications.		X
Provide specific software/hardware recommendations to enhance existing System Security, Configuration, and Performance issues.		X
Provide BlackBerry administration, database, and technical support services to IO.		X
Management of Wallace Incident Communicator (WIC) and Metamessage applications and associated servers		X
Configure and maintain GSA BlackBerry Infrastructure from the Central Office in Washington D.C.		X
Provide BlackBerry technical support to regional local support staffs for installation and troubleshooting to GSA nationwide.		X

<b>BlackBerry Technology Support</b>	<b>Government</b>	<b>Contractor</b>
Provide immediate reporting on known security threats and virus updates to the Government. Additionally, the Contractor shall implement security patches/fixes to mitigate risk.		X
Design and implement a BlackBerry Test Laboratory for the purpose of providing a demonstration and testing environment for GSA nationwide. Laboratory personnel will coordinate testing of new products in coordination with both GSA Service and Staff Office personnel and the GSA Information Technology Architectural Planning Committee (ITAPC).		X
Provide BlackBerry Administration and DBA/Application support which includes but not limited to: add/delete user accounts; backup/recovery; account management; installation/integration of software; password management; monitoring for performance and availability		X
Perform DBA operation/technical functions; maintain system documentation, and hardware/software configuration on the BlackBerry and support systems.		X
Provide technical support to maintain, upgrade, install, and test BlackBerry Infrastructure Equipment, performing the following specific duties and functions:		X
<ul style="list-style-type: none"> <li>• Inventory and track all incoming BlackBerry devices through the standardized ERM framework.</li> </ul>		X
<ul style="list-style-type: none"> <li>• Prepare, pack, and ship inventory hardware and software, with its associated documentation when available, to CIO regional offices, as directed by the Government.</li> </ul>		X
<ul style="list-style-type: none"> <li>• Manage inventory of new/used/defective/obsolete equipment.</li> </ul>		X
Provide immediate reporting on known security threats and virus updates to the Government. Additionally the Contractor shall provide immediate follow-up and recommendations to the Government.		X
<b>Configuration Management/Change Control</b>		
Define configuration management and change control policies and procedures.	X	
Perform configuration management and change control activities throughout life cycle of support services.	X	X
Approve change control results.	X	
Operate and maintain a collection of software packages and scripts.	X	X
<b>Monitoring and Reporting</b>		
Approve and document service levels and reporting cycles.	X	

<b>BlackBerry Technology Support</b>	<b>Government</b>	<b>Contractor</b>
Measure and analyze performance relative to requirements.		X
Develop improvement plans where appropriate.		X
Implement improvement plans.		X
Report on service level performance results.		X

5.4.5. Place of Performance

The place of performance shall be government offices at GSA, 1800 F Street, Washington, D.C.

5.4.6. Hours

These services will normally be performed during the core work hours of 7:00 AM to 7:00 PM, Monday through Friday. However, the Contractor may be required to work outside the core work hours in response to emergency requirements. Also, occasional overtime support and on-call coverage may be required (this includes the weekend, early morning hours, late evening hours, and Federal holidays).

5.4.7. Effort Estimate

Historically the effort to fulfill the requirements described in Table 4.7 -1 BlackBerry Services Requirements has been 10 FTEs.

**6. DESKTOP MANAGEMENT**

**6.1. Software Deployment**

6.1.1. Background And Technical Environment

6.1.1.1. GSA Software Deployment Services enables the automated deployment of software via an enterprise management tool set to one or more customers, workstations or servers. The customer has the option to accept distributed software at their convenience, with the exception of mandatory pushes including security or critical systems patches. Software Deployment is responsible for the automated deployment of applications, patches, Office Suite and virus updates, and all associated processes including creation, coordination, testing and distribution of deployment packages and software deployment applications.

6.1.1.2. Software deployment tools within GSA include WinInstall, CA Unicenter, distributed self deployment applications, maintenance of the deployment tools and utilities themselves, integration of the deployment tools with the server and client environments, reporting of success/failures, tracking of

software licenses, etc. Approximately 75 percent of GSA utilizes Computer Associates (CA) suite to provide desktop management, including remote control, software/hardware inventory, and automated installation services. The remaining 25 percent utilizes a suite of products to accomplish the same desktop management services. This suite consists of Proxy remote control, WinInstall Asset Management, and WinInstall Software Distribution Management. GSA supports both Enterprise (tethered) and Remote (dialup) users. The ability to provide software management and asset management, either through network access or remote CD software distribution, is currently supported through the OnDemand WinInstall suite of utilities. Together, this suite of tools is used to manage desktops across the GSA enterprise.

#### 6.1.2. Objectives

- 6.1.2.1. The Contractor must support the current automated installation tool sets within the GSA infrastructure. The objective of automated deployment services is to provide automated deployments to all GSA users via a standardized solution. Automated installation packages should, on average, require no longer than three business days to build, test and begin deployment. However, the Government may designate certain installation packages as “Emergency Releases.” In such a case, the vendor is expected to have such releases prepared and ready for release in no more than 36 hours.
- 6.1.2.2. Support application developers, Security and other offices within GSA by consistently Building and deploying distribution packages.
- 6.1.2.3. Support asset management and reporting requirements enterprise wide for all IT assets.

#### 6.1.3. Scope

- 6.1.3.1. Comprehensive software deployment, asset management and reporting will be accomplished using a standardized approach and standardized suite of tools as opposed to the multiple approaches and tools currently being used throughout the agency to accomplish this work. However, the Contractor must support the legacy automated installation tools. See Attachment-22 for listing of automated installation tools.

#### 6.1.4. Requirements

- 6.1.4.1. The Contractor shall be responsible for supporting the legacy

automated installation tools in GSA while assisting with the planning and migration efforts to a standardized automated deployment tool. Strategies will include distributing software via a standardized enterprise management tool set. Software will be deployed to one or more customers, workstations or servers based explicitly on requirements or implicitly on policy settings. The customer will have the option to accept distributed software at their convenience. Conversely, the customer, workstation and server will accept mandatory software as distributed. The work items include:

**Table 3.1.4.1 REQUIREMENTS MATRIX**

<b>Software Deployment</b>	<b>Government</b>	<b>Contractor</b>
<b>Operations and Administration</b>		
Research and analyze development of packages and scripts to distribute software		X
Define requirements	X	
Identify possible product enhancement opportunities for improved performance and potential cost savings	X	X
Approve projects to implement product enhancement opportunity	X	
Design, develop, operate, maintain and enhance (keep current) a test environment emulating the operating workstations and servers	X	X
Distribute software packages via the enterprise management tool set		X
Test new releases of supported software to ensure conformance with GSA service level requirements		X
Install new releases of supported software on servers and standalone/mobile PCs		X
Initialize desktop devices, as needed, in conjunction with migration/upgrade		X
Verify desktop is fully functional following the migration/upgrade process		X
Provide technical assistance during conversion as requested		X
Develop and maintain a comprehensive set of procedures to distribute each software package		X
<b>Software Management</b>		
Establish software license management policies	X	
Establish supported software portfolio	X	
Negotiate and procure software site or individual licenses that protect GSA right to use the software	X	
Track software assets (user, location, asset id, finances)		X
Maintain software product inventory as needed		X

<b>Software Deployment</b>	<b>Government</b>	<b>Contractor</b>
Establish software migration/upgrade standards and policies	X	
Develop detail procedures to ensure low-risk migration/upgrade		X
Test new releases of supported software to ensure conformance with GSA service level requirements		X
Install new releases of supported software on servers and standalone/mobile PCs		X
Initialize desktop devices, as needed, in conjunction with migration/upgrade		X
Verify desktop is fully functional following the migration/upgrade process		X
Provide technical assistance during conversion as requested		X
Provide technical assistance during conversion as requested		X
<b>Configuration Management/Change Control</b>		
Define configuration management and change control policies and procedures	X	
Document Policies, Procedures, change requests and activities		X
Perform configuration management and change control activities throughout life cycle of support services		X
Approve change control results	X	
Operate and maintain a collection of software packages and scripts		X
<b>Monitoring and Reporting</b>		
Approve and document service levels and reporting cycles	X	
Measure and analyze performance relative to requirements		X
Develop improvement plans where appropriate		X
Implement improvement plans		X
Report on service level performance results		X
<b>Chargeback</b>		
Assign user account codes	X	
Maintain table for GSA account codes		X
Track utilization		X
Produce cost center invoices		X
Send invoices		X
Respond to GSA inquires		X

## 6.2. Client Engineering Services

### 6.2.1. Background And Technical Environment

6.2.1.1. The General Services Administration (GSA), Office of the GSA Chief Information Officer (I) has installed and integrated

standards based personal computers throughout the GSA enterprise. Distributed computing hardware resources include networked and non-networked personal computer (PC) systems (e.g., desktop, tower, workstation and laptop computers). Peripheral devices include personal printers, scanners, PDAs, headsets, external storage devices and other similar devices. These PCs are connected into the GSA Wide Area Backbone Network (WABN). The GSA WABN is a robust ATM network with the majority of field locations linked in via T-1, DSL, EDSL, ISDN or 56kb circuits. Microsoft 2000 and 2003 Servers are located in each of the regions as well as Central Office locations and at various field office locations. They are used to support applications, file and print, DHCP, WINS, and Desktop Management services. The total number of Windows based application servers is provided in Attachment-1. GSA has a substantial investment in Net App network area storage servers as well. These servers are present in all GSA Regions and within GSA Central Office locations. These devices are primarily used for file server services and also are lynch pins of GSA's Continuity of Operations Plan (COOP).

- 6.2.1.2. A standard suite of Office Automation software, as well as business critical applications such as FSS19, the Fleet Management System, the Customer Supply Center System, System for Tracking and Administering Real Property (STAR), Occupancy Agreement Tool (OA Tool), Pegasys Financial System, IT Solutions System (ITSS), and others are provided to GSA associates. GSA's approximately 15,000 users depend on these services to be operational in order for them to perform their work. These employees are located in the GSA regional cities, the 400 Property Management Offices, the two GSA distribution centers, the 130 GSA fleet management centers, the 11 GSA Customer Supply Centers, 10 GSA remote field offices, 6 sites in Germany, 10 sites in Asia, Crystal City, VA, Springfield, VA, McLean, VA, Washington, D.C. See Attachment-2 for a complete list of locations.
- 6.2.1.3. The current GSA distributed computing architecture is standardized on Windows XP Professional. GSA currently engages contractor support personnel to complement its client service efforts. It includes support for new installations, break-fix and upgrades.
- 6.2.1.4. The client hardware utilized by GSA includes, but is not limited to, Compaq, Dell, and Hewlett Packard. The

overwhelming majority of laptops and desktops are Dell equipment. The majority of this equipment is refreshed every three years. The distributed computing environment (DCE) also includes personal/local printers, scanners and other peripherals. (See Attachment-3 for a full listing of hardware and Attachment-8 for GSA standard image software).

#### 6.2.2. Objectives

- 6.2.2.1. The objective of this sub-task is to provide technical support services in the areas of client services to include small and large computer deployments, image management, desktop management and SME support for the General Services Administration. This support will be used to deploy new systems and operate and maintain existing GSA client services. The desktop infrastructure consists of laptops, desktops, docking stations, PDAs, peripheral devices, management and reporting systems and associated software.
- 6.2.2.2. The solution used by the Contractor must either be capable of interfacing with current ticketing systems and/or be quickly deployed across the GSA enterprise so as to avoid a lengthy enterprise management transition period.
- 6.2.2.3. GSA seeks to achieve a greater degree of standardization particularly in the areas of client side configuration and client deployment services.
- 6.2.2.4. GSA further wishes to move toward a more centralized client support model through the improvement of image management and distribution services.

#### 6.2.3. Scope

- 6.2.3.1. GSA requires client engineering services support to coordinate and complete enterprise-wide PC deployments, large scale moves/adds/changes, provide conference support, asset management support, creation/change management and quarterly update and distribution of GSA's client image, and sets policies and design procedures to carry out such support activities. Other services required include researching new technologies to enhance GSA's desktop client infrastructure, operations and administration, configuration and change control management, SME (on-site and off-site) technical support related to desktop management and remote access client support to all the end users in GSA. The overwhelming majority of GSA users utilize personal computers; however,

there is a very small contingent of Apple personal computers in use at GSA for which these services will also be required. See Attachment-1 for hardware inventory.

- 6.2.3.2. GSA OCIO provides and manages the standard GSA client image to be used throughout the agency. Client operating system updates and office suite updates and support are also provided by OCIO. Equipment and software components are subject to change based on technological advances. This group assists the Government in evaluating, upgrading, or replacing new hardware/software. The client engineering services group coordinates with all offices within the Office of Enterprise Infrastructure to ensure a robust knowledge/skill base, capable of supporting all aspects of the PC is maintained.

#### 6.2.4. Requirements

##### 6.2.4.1. Image Management

- 6.2.4.1.1. The Contractor shall provide the standard desktop image for GSA. Standard images shall be installed on the new desktop and laptops and updated quarterly. Updated images shall be provided quarterly to GSA systems staffs.
- 6.2.4.1.2. These images shall include updated standard configuration and GSA specific applications required on the user desktops.
- 6.2.4.1.3. Individual users PCs are further customized through the use of automated software push.

##### 6.2.4.2. GSA Standard Image

- 6.2.4.2.1. The Contractor shall develop and provide support services for the GSA Standard Images to include the Windows XP Professional and Windows XP Tablet edition.
- 6.2.4.2.2. The standard configuration of GSA desktops is provided in Attachment-8.
- 6.2.4.2.3. *Note:* All Microsoft updates are applied to the release within a week of the release date. Windows Automatic Updates are, by default, enabled in the Standard Image. Updates include all Microsoft application software (e.g., MS Office, Visio, MS Project, etc.).

##### 6.2.4.3. Conference Support and Large Scale Moves, Adds, and

## Changes (MACs)

- 6.2.4.3.1. GSA organizes a number of conferences throughout the year. Conferences may be tasked to local support if they are not national in nature, and if they require simple client configurations and/or involve less than 500 participants, Events whose characteristics fall outside of those previously described shall be supported under this sub-task.
- 6.2.4.3.2. GSA OCIO currently supports the Election Assistance Commission (EAC) for its messaging needs. Also, once every four years, it is necessary to provide electronic messaging support for the Presidential Transition Team (PTT). There is also a government-owned and operated off-site location with redundant hardware/software that can be put into service in the event of extended downtime of multiple sites or locations. Test, staging and evaluation environments are also maintained and utilized by the team constantly in support of the infrastructure environment.
- 6.2.4.3.3. MACs, which involve ten or fewer workstations, are the responsibility of local support. For these MACs users or Move Coordinators will contact the GSA National Help Desk for support of individual moves. However, large scale moves such as office relocations, building moves, field site moves and the like shall be provided for within this sub-task. The Contractor shall designate personnel to perform the following tasks in support of GSA conferences and other large moves, adds, and changes (MACs) as specified in this sub-task:
  - 6.2.4.3.3.1. Ensure MAC operations are performed with minimum disruption in day-to-day functioning of the users.
  - 6.2.4.3.3.2. Coordinate refresh cycles.
  - 6.2.4.3.3.3. Ensure proper documentation is available for technical personnel and end users.
  - 6.2.4.3.3.4. If tasked by GSA, contact hardware contractors and follow up on the

break-fix of the items under warranty.

6.2.4.3.3.5. The Contractor provided Move-Add-Change (MAC) services include:

- i. Move: The Contractor shall disconnect the installed unit and its external devices and, after packaging, move them to a new location, and unpack, reconnect, and test the unit, and its external devices, in its new location. This may include coordinating with other groups for network connectivity in the new location and on-site user orientation.
- ii. Hardware Add: Attach a new external device, such as an external modem, disk drive, printer, or scanner, and install the appropriate device driver to an existing unit.
- iii. Software Add: Install new software using server-based or CD distribution. This should be rare as GSA prefers the use of automated installation wherever and whenever possible.
- iv. Hardware Change: Upgrade (adding functionality), downgrade (removing functionality), or change an existing hardware unit and associated device drivers, and test for network connectivity.
- v. Software Change: Set up a user's system, including putting network icons on the Desktop or customizing an application, and test for network connectivity and function.
- vi. Remove: Disconnect a unit and

external devices and, after packaging, move them to an on-site defined storage location.

- vii. Refresh: Provide a new system to a user by removing an existing unit and its external devices and installing a new system as needed or dictated by changing needs at GSA.
- viii. Cascade: Move assets among users in either successive refreshes or a new installation and a refresh.

6.2.4.3.4. The Contractor shall monitor and document physical (e.g., equipment) and logical (e.g., IP address) moves, adds, changes, installations and re-installations, regardless of the number of users, instances and/or systems.

#### 6.2.4.4. Hardware Refresh Cycle

6.2.4.4.1. GSA's refresh cycle for desktop and laptop PCs is begun every third year and completed in year four. The Contractor shall assist OCIO with enterprise-wide hardware refresh deployments. The Contractor shall assist with testing and installation of all client-side large-scale hardware / software deployment efforts. GSA expects the Contractor to coordinate these large scale refresh activities with local support in order to augment resources necessary to complete this work effort in a timely manner. Even with this coordination / augmentation, it is likely this effort will require the employment of competent temporary surge resources.

#### 6.2.4.5. Workstation Data Backup

6.2.4.5.1. Data backup on personal computers and laptops is considered a *user responsibility*. Users are aware of their data storage responsibilities and are allocated fault tolerant fully backed up storage space on file servers. Thus, no requirement exists for desktop data backup and retrieval (the exception to this rule

would include refreshing equipment which may require backup and retrieval).

6.2.4.6. Special System Requirements

6.2.4.6.1. Office Automation Applications and Utilities: Office Automation Applications include but are not limited to: Microsoft Office, Lotus Notes, calendaring, news service access and display, web browser, collaboration and document sharing, etc. A complete standard software configuration is included in Attachment-8. The Contractor shall designate personnel to perform the following work items in support of the GSA common suite of centralized workstation tools as specified in this sub-task:

6.2.4.6.1.1. Installation and upgrades.

6.2.4.6.1.2. Troubleshooting of any issues arising from upgrades.

6.2.4.6.1.3. High level support and coordination.

6.2.4.6.1.4. Helpdesk ticket management.

6.2.4.6.1.5. Research and testing for future upgrades.

6.2.4.6.1.6. Remote access utilities installed on the assets under this sub-task.

6.2.4.6.2. Desktop Management: The Contractor shall designate personnel to perform the following work items in support of the GSA desktop management services specified in this sub-task:

6.2.4.6.2.1. Remote Control

i. Administration

ii. Configuration

iii. Agent deployment

iv. Troubleshooting

v. Integration with the Helpdesk systems

6.2.4.6.2.2. Software/Hardware Inventory

i. Administration

- ii. Configuration
  - iii. Agent deployment
  - iv. Troubleshooting
  - v. Integration with finance and/or Helpdesk systems
- 6.2.4.6.2.3. Asset Management
- i. Administration
  - ii. Configuration
  - iii. Agent deployment
  - iv. Troubleshooting
  - v. Integration with finance and/or Helpdesk systems
- 6.2.4.6.2.4. Automated installation services
- i. Administration
  - ii. LAN and Remote Package creation
  - iii. Configuration
  - iv. Agent deployment
  - v. Troubleshooting
  - vi. Integration with Helpdesk and/or reporting systems

**Table 3.2.4.1 REQUIREMENTS MATRIX**

<b>Client Engineering</b>	<b>Government</b>	<b>Contractor</b>
<b>Operations and Administration</b>		
Define Desktop/end user capability requirements	X	
Define services and standards for desktop/end-user capabilities	X	
Identify possible product enhancement opportunities for improved performance and potential cost savings	X	X
Approve projects to implement product enhancement opportunity	X	
Identify possible product enhancement opportunities for improved performance and potential cost savings	X	X
Provide input processing support for activities such as loading media, receiving batch electronic file transmissions, etc.		X
Define automated output distribution requirements		X

<b>Client Engineering</b>	<b>Government</b>	<b>Contractor</b>
Create standard GSA infrastructure profiles specific to IT service area (e.g., desktop profiles for distributed computing)		X
Develop scripts and macro programs to automate standard GSA processes as appropriate (e.g., upgrading desktop profiles)		X
Provide high level support for desktop hardware and software		X
Approve construction/development plans and procedures where there is an impact on other GSA entities/facilities and/or other GSA third party agreements.	X	
<b>Configuration Management/Change Control</b>		
Define configuration management and change control policies and procedures	X	X
Document Policies, Procedures, change requests and activities		X
Perform configuration management and change control activities throughout life cycle of support services		X
Approve change control results	X	
<b>Image Management</b>		
Identify the software to be included in the standard image	X	
Develop image CDs		X
Update the associated documentation		X
Installation of image		X
<b>Office Moves and Other Large scale MACs</b>		
Disconnect, pack and ship the units to new location		X
Unpack, reconnect, test units and attached devices at new location and install them		X
Perform hardware add and change at end user location		X
Perform network based or CD distribution for software change and add		X
<b>Monitoring and Reporting</b>		
Approve and document service levels and reporting cycles	X	
Measure and analyze performance relative to requirements		X
Develop improvement plans where appropriate		X
Implement improvement plans		X
Report on service level performance results		X
<b>Chargeback</b>		
Assign user account codes	X	
Maintain table for GSA account codes		X
Track utilization		X
Produce cost center invoices		X
Send invoices		X
Respond to GSA inquires		X

### 6.3. Server Services

#### 6.3.1. Background

The GSA OCIO requires technical, administrative and operational support services for GSA's server management infrastructure supporting operations and applications systems across GSA. The current operational support and other services required to support these servers is distributed within GSA to each Service, Staff office and/or region. Each office provides management and operational support of the server infrastructure within their customer base. The operating systems and hardware configurations are specified by the GSA wide standards outlined within the TRM (Technical Reference Manual), Attachment-4. However, these services are provided by the individual offices whose needs and procedures may vary. The server administration and management services these organizations provide includes, but may not be limited to, backup/restore, policy, procedures deployment, patch management, security, and overall management as well as COOP support. These systems support a wide range of operational functions and applications systems. GSA OCIO provides management and administration support for the GSA Headquarters building and Staff offices within the GSA HQ facility. FSS provides a centralized model supporting the entire FSS enterprise including FSS CO, FSS regional offices and field locations. PBS maintains a distributed support model in which each of its regional offices provides management and support of the servers in that region. Most of FTS' server support is provided by individual regional PBS IT support staff in the regions. FSS supports FTS' servers in regions 2 and 10 centrally from FSS HQ. FTS HQ provides server support for FTS HQ servers. FTS regions 4, 5 and 8 provide support for servers located in each of these regions.

#### 6.3.2. Objectives

- 6.3.2.1. GSA OCIO wishes to implement an IT infrastructure consistent with industry best practices and expects the Contractor to provide a comprehensive, best value solution for contracted services.
- 6.3.2.2. GSA OCIO realizes that the implementation and provisioning of Server Services in accordance with industry best practices will not occur over night. Thus, the Government wishes to provide support for its assets requiring Server Services in the manner in which it is currently provided.
- 6.3.2.3. GSA OCIO understands that the current support of the server infrastructure, hosting applications and operational systems requires a more centralized approach in order to obtain desired efficiencies. GSA wishes to centralize the infrastructure

support, based on industry best practices, thereby reducing the effort and cost required to manage and house the server environments. GSA wishes to provide a centralized and consolidated technical approach in the areas of server services to include small and large server deployments, standards based build/image management, server management and high level support of the GSA environment and customer base. This support will consist of both maintenance and enhancement; i.e., operation and maintenance of existing GSA servers and deployment of new servers as well as strategic consolidation efforts of these systems. GSA expects to stay current on Operating System platforms and maintain the integrity of the operational and application systems this environment supports.

6.3.2.4. GSA intends to:

- 6.3.2.4.1. Deploy a centralized standards based security and patch management solution.
- 6.3.2.4.2. Enhance application availability for end-users both locally and remotely by providing a secure, reliable, stable, and efficient infrastructure supporting the operations and application systems.
- 6.3.2.4.3. Reduce administration, support and operational costs of GSA's Server Infrastructure and methods of managing this environment.
- 6.3.2.4.4. Provide GSA system and application owners with the tools and rights required to manage the environments without negatively impacting the integrity of the shared systems.
- 6.3.2.4.5. Provide a comprehensive enterprise backup solution.
- 6.3.2.4.6. Increase remote management of server resources.
- 6.3.2.4.7. Establish and implement a strategic plan resulting in the appropriate consolidation of shared resources.

6.3.3. Scope

- 6.3.3.1. Support for these services consists of system installation, configuration, administration, maintenance, upgrade, enhancement, monitoring, backup/restore and management of GSA's Operation and application systems. GSA is standardized on several platforms (See Attachment 4, GSA

TRM) and requires centralized support for these systems based on application and operational requirements. In addition, upgrades to the Operating systems, server platform, and enhancements will be required to support GSA operational and application system resources. The server infrastructure consists of all flavors of Microsoft Operating Systems from NT to 2003, Linux, and Unix platforms. File services are not centralized and include support for MS Windows based file servers, NAS and SAN environments. Hardware support is required for a diverse base of platforms; some include Dell, HP, Sun Solaris and Network Appliance (See Attachment 1 for Inventory). GSA has a large investment in Network Appliance for file services; this investment has been made by several of the Services and Staff offices. Included in the support for server services will be peripheral devices, management and reporting systems and associated software. The server systems supporting GSA are located in various regions and sites within GSA; remote management is leveraged day to day. A longer term goal is a review of the server distribution, with the desire to further consolidate servers where it makes business sense. GSA's primary focus is the creation of an architecture and implementation plan resulting in a centralized and consolidated management model of server assets which will yield a more standardized and efficient service.

6.3.3.2. GSA requires 24x7 technical support services for its production Server Services infrastructure and core hour support for all other environments, which include test, development and staging. Systems making up this infrastructure are located at GSA headquarters and 11 regional office locations and field sites. Headquarters and the regional offices locations include Washington, DC; Boston, MA; New York, NY; Philadelphia, PA; Atlanta, GA; Chicago, IL; Kansas City, MO; Fort Worth, TX; Denver, CO; San Francisco, CA, and Auburn, WA. (See attachments 1,1a and 2, for detailed location information) The Contractor shall assist the Government in consolidating server resources and deploying and maintaining an enterprise server services environment.

6.3.3.3. NOTE: File and Application servers are present at many remote field locations. GSA Server infrastructure ranges from File Services to utility servers such as DHCP, DNS and WINS, Enterprise resource management services such as automated deployments, asset management and reporting tools, Document Management such as Documentum and Share Point, Database

servers such as Access, SQL, MySQL (Open Source), Oracle and Sybase, Application Servers running various Cots packages, web servers including IIS and Apache. These services run on various system architectures with multiple redundancy approaches such as clustering and load balancing. The various resources and architectures above do not represent a comprehensive inventory of technologies requiring support within GSA. They are intended to demonstrate the diverse technical offerings which require support within GSA.

6.3.4. Requirements

- 6.3.4.1. Technical support is necessary to deploy new systems and operate, maintain and enhance the existing GSA distributed server services environment. Support is also required to manage operations and changes to the existing GSA server services infrastructure. GSA requires technical support to provide solutions for GSA customer base server requirements. These efforts include support for new installations, break-fix and upgrades. The Contractor will achieve GSA's efficiencies and cost savings targets through the implementation of a centralized and consolidated support model for the server services infrastructure. This infrastructure will include support for enterprise wide backup management, file and print services, system management and day to day administration of utility and application servers.
- 6.3.4.2. Servers currently supported centrally will continue to be supported in such a manner. The Contractor will provide support necessary for servers that are not supported centrally using Local Support when necessary. In other instances, full time, on-site personnel may be required. As GSA evolves toward best practices, a more consolidated infrastructure and a more centralized management model; the Contractor will provide more and more required server support centrally.
- 6.3.4.3. Details of server locations, quantity, types, and management model provided for these servers are included in Attachment 1a. The users depend on GSA server services to be operational in order for them to perform their work. Approximately 15,000 GSA employees utilize server services for access to resources providing support to the business application systems and operational support. Employees and systems are located across the country and a small presence in Europe and Asia (See Attachment 2).

**Table 3.3.4.1 Typical Work Items Associated with Server Services**

<b>SERVER SERVICES</b>	<b>Government</b>	<b>Contractor</b>
<b>Server Administration and Operations</b>		
Provide 24x7 days monitoring, reporting and support services for the services required		X
Provide a standards base build and automated procedure for each platform supported. Security guidelines need to be included in the base builds		X
Integration support		X
Provide performance reports on consolidated environments. (e.g. processor utilization, memory allocation and usage, drive space usage)		X
Provide system and engineering support to development and helpdesk groups within GSA		X
Provide day to day administration and management support for managed systems		X
Server Builds		X
Vulnerability assessments		X
Perform LAN administration to include file and print sharing, logon user-id and password maintenance		X
Configure, set up and monitor servers with Operating system and network operating system		X
Monitor, report and analyze server performance statistics		X
Identify possible product enhancement opportunities for improved performance and potential cost savings	X	X
Test, install, tune technical environment hardware, software, peripherals & services.		X
Approve projects to implement product enhancement opportunity	X	
Build and maintain lab environment		X
<b>Data Backup and Recovery</b>		
Recommend backup/recovery requirements		X
Approve backup/recovery requirements	X	
Perform periodic incremental and full tape backups		X
Exchange backup tapes with storage facility		X
Provide input processing support for activities such as loading media, receiving batch electronic file transmissions, etc.		X
Mount and remove tape volumes as needed		X
Maintain a tape library, tape management system and transport tapes to production area as needed		X
<b>Maintenance</b>		
Define maintenance and repair policies and procedures	X	

<b>SERVER SERVICES</b>	<b>Government</b>	<b>Contractor</b>
Perform diagnostics on hardware, software, peripherals and services (as appropriate)		X
Install manufacturer field change orders, IS security patches, service packs, firmware and software maintenance releases, BIOS upgrades, etc.		X
Perform software distribution and version control, both electronic and manual		X
Replace defective parts and systems, including preventive maintenance according to the manufacturer's published mean-time-between failure rates		X
Conduct maintenance and parts management and monitoring during warranty and off-warranty periods		X
Perform routine system management e.g., system tuning. In compliance with FSS defined schedule		X
Perform maintenance on peripherals and special purpose devices		X
<b>Technical Support</b>		
Participate in defining technical support policies and procedures	X	X
Provide tier 3 technical support; as requested.		X
Dispatch repair technicians to the point-of-service location	X	X

#### **6.4 Thin Client (Administration And Operation Of The WTS/Metaframe)**

##### **6.4.1 Background**

GSA has a distributed WTS/Citrix Metaframe environment, which is currently supported in a decentralized manner. Most organizations within GSA, with the exception of Region 1, primarily leverage WTS/Citrix Metaframe for remote access to GSA systems and applications. Region 1 utilizes Citrix for day to day support of operations, access to almost all business applications and as a key piece of their COOP environment.

6.4.1.1 Support for this technology consists of server installation, configuration, administration, maintenance, upgrade, enhancement, monitoring, and operation of GSA's Thin Client environment as it exists today. Current staffs are responsible for regular application additions, upgrades, modifications and performance tuning to the thin client platform as well as enhancements for the end user remote access to GSA operational resources.

6.4.1.2 A longer term goal is a review of the Metaframe server distribution, with the desire to further consolidate servers where it makes business sense. GSA's vision is the creation of

an efficient architecture and associated implementation plan, which results in a centralized and consolidated management model of Thin Client assets

6.4.2 Objectives

To operate and maintain the GSA Thin Client infrastructure and facilitate the evolution of that infrastructure to meet GSA’s Thin Client vision.

6.4.3 Scope

6.4.3.1 GSA requires technical support services for its WTS/Citrix Metaframe infrastructure. Systems making up this infrastructure are located at GSA headquarters, Federal Supply Service Headquarters, Federal Supply Service Headquarters as well as 11 regional office locations. Headquarters and the regional offices locations include Washington, DC; Willow Wood, Va., Crystal City, Va., Boston, MA; New York, NY; Philadelphia, PA; Atlanta, GA; Chicago, IL; Kansas City, MO; Fort Worth, TX; Denver, CO; San Francisco, CA, and Auburn, WA. Every region has deployed and currently maintains their own environment for support of remote access to applications and drive mappings to shares located on file servers.

6.4.3.2 The following table provides the details on the size and scope of the current Metaframe server installations:

**Table 3.3.4.2-1 Citrix Assets**

<b>REGION</b>	<b>CITRIX Server Assets</b>	<b>Tools &amp; Utilities</b>	<b>CITRIX Licenses</b>	<b>CITRIX Secure Gateway/WEB Interface</b>	<b>No. of APPS</b>	<b>PRIMARY USE</b>	<b>Contract hours / year</b>
1	8 Production Servers @ ROB, 1 DataStore Server @ ROB, 4 Production Servers @ COOP location	Provision Networks Print-IT	400 PS 4 (SA)	1 @ ROB, 1@ COOP site	55	Tele-work, COOP, Field Office Support, Notes E-mail portal for enterprise	1,000

<b>REGION</b>	<b>CITRIX Server Assets</b>	<b>Tools &amp; Utilities</b>	<b>CITRIX Licenses</b>	<b>CITRIX Secure Gateway/WEB Interface</b>	<b>No. of APPS</b>	<b>PRIMARY USE</b>	<b>Contract hours / year</b>
2	4 Production Servers @ ROB, 2 Production Servers @ COOP location	NONE	120 PS4 (SA)	1 @ ROB, 1@ COOP site	30	Tele-work, COOP, Field Office Support,	1,000
3	3 Production Servers @ ROB, 1 Production Servers @ COOP location	None	200 PS4 (SA)	none, (planned)	100	Tele-work, COOP, Field Office Support, National Application	1000
4	20 Production Servers @ ROB, 2 Production Servers @ COOP location	EOL Universal Printer	980 PS 4 (SA)	1 @ ROB, 1@ COOP site	40	Tele-work, COOP, Field Office Support, Notes E-mail portal for enterprise	2000
5	3 Production Servers @ ROB, 2 Production Servers @ COOP location	EOL Universal Printer	400 PS3 (SA)	1 @ ROB, 1@ COOP site	20	Tele-work, COOP, National Apps (Field Office Support Planned)	1000

<b>REGION</b>	<b>CITRIX Server Assets</b>	<b>Tools &amp; Utilities</b>	<b>CITRIX Licenses</b>	<b>CITRIX Secure Gateway/WEB Interface</b>	<b>No. of APPS</b>	<b>PRIMARY USE</b>	<b>Contract hours / year</b>
6	8 Production Servers @ ROB, 1 Data Collector	Thin Print	370- PS4 (SA)	1 @ ROB	30	Tele-work, COOP, Field Office Support, Notes E-mail portal for enterprise	1,500
7	9 Production Servers @ ROB, 1 Production Servers @ COOP location	None	745 PS4 (SA)	1 @ ROB, 1@ COOP site (planned)	70	Tele-work, COOP, Field Office Support, Notes E-mail portal for enterprise	1200
8	5 Production Servers @ ROB, 2 Production Servers @ COOP location	Print-IT	50 PS4 (SA)	1 (WI) @ ROB 1(WI) @ COOP	20	Tele-work, COOP, Field Office Support, Notes E-mail portal for enterprise	1500
9	9 Production Servers @ ROB	Print-it	350 Xpe (SA)	1 @ ROB	20	Tele-work, Field Office Support, National Application	1000

<b>REGION</b>	<b>CITRIX Server Assets</b>	<b>Tools &amp; Utilities</b>	<b>CITRIX Licenses</b>	<b>CITRIX Secure Gateway/WEB Interface</b>	<b>No. of APPS</b>	<b>PRIMARY USE</b>	<b>Contract hours / year</b>
10	5 Production Servers @ ROB, 1 Production Servers @ COOP location (planned)	EOL Universal Printer & screwdrivers	325 Xpe (SA)	Not currently but planned	10	Tele-work, Field Office Support, PBS National Aps	1000
11	2 Production Servers @ ROB, 1 Production Servers @ COOP location	Uniprint Print Server	180 Metaframe Presentation server 4.0	N/A	30	Tele-work, Field Sites, Notes E-mail.	520
FSS CO	2 Production Servers @ ROB	TriCerat printing util.	155 - PS 3.0 (SA)	1 @ CO	21	Tele-work, Field Office Support, Notes E-mail portal for enterprise, external users	500
FTS CO	4 Production Servers @ ROB, 3 Production Servers @ COOP location	screwdrivers	100 PS4 (SA)	1 WI	40	Tele-work, Field Office Support, National Aps	1500

<b>REGION</b>	<b>CITRIX Server Assets</b>	<b>Tools &amp; Utilities</b>	<b>CITRIX Licenses</b>	<b>CITRIX Secure Gateway/WEB Interface</b>	<b>No. of APPS</b>	<b>PRIMARY USE</b>	<b>Contract hours / year</b>
OCIO	15 Production Servers @ ROB, 4 Production Servers @ COOP location, 1DB server	None	150 Xpe & PS4 (SA)	2 WI	15	Tele-work, COOP	2000
FINCEN	6 Production Servers @ ROB, Production Servers @ COOP location	none	800 PS4 (SA)	2 WI	30	FEDDESK, ETAMs	3000

#### 6.4.4 Requirements

The Contractor shall support GSA’s current Thin Client infrastructure. The Contractor shall conduct an evaluation of this infrastructure and propose a plan to evolve this infrastructure to a more efficient model. The Contractor shall support daily administrative works related to WTS/Citrix Metaframe implementations. Provide tier 2/3 support for the engineering of the new architecture as well as resolution of tickets in the standardized ERM framework. Troubleshoot server problems and issues. Contact end users and troubleshoot Citrix connection issues. Triage and escalate issues as necessary. The Contractor shall provide resources with knowledge and skills necessary to support Windows Terminal Services, Citrix Metaframe (including versions Metaframe XP, Metaframe Presentation Server, and future versions as defined by the government), and Citrix Nfuse/secure Web Interface. The Contractor shall also provide support for various thin client (Windows CE or embedded Windows XP) terminals primarily used for kiosk or COOP installations.

**Table 3.3.4.2 - 2 Typical Work Items Associated with Thin Client Services**

<b>Thin Client</b>	<b>Government</b>	<b>Contractor</b>
<b>Operations and Administration</b>		
Support Thin Client Infrastructure 24x7		X
Provide on-call support outside of core hours		X
Project Management Oversight	X	
Project Management Support		X
Provide Software Maintenance Support		X
Standard Operating Procedures Development and Maintenance	X	X
Define system capability and requirements	X	X
Define services and standards for remote desktop/end-user capabilities	X	X
Define standard client configuration criteria for Thin Client	X	X
Plan, Analyze, Design and implement Centralized solution	X	X
Develop Farm and Load Management designs		X
Implement Profile management and login scripts		X
Test and secure access to system and applications		X
Develop and document design, environment and test procedures		X
Integrate GSA applications and resources required for support on Thin Client systems		X
Train regional and local staff in proper configuration and deployment practices		X
Identify possible product enhancement opportunities for improved performance and potential cost savings	X	X
Support the development of scripts to automate standard GSA processes as appropriate for client access to resources/applications		X
Provide Tier 2/3 support for Thin Client solutions		X
<b>Configuration Management/Change Control</b>		
Define configuration management & change control policies and procedures		X
Perform configuration management & change control activities throughout life cycle of support services		X
Approve change control results	X	
<b>Training Activities</b>		
Establish training plans and procedures	X	X
Provide advanced training, as agreed, to GSA technical personnel to facilitate full exploitation of all relevant functional features		X
Provide training for GSA personnel to improve “how-to-use” skills related to IT service area systems and applications		X
Provide distributed computing support for classrooms, labs and electronic learning events		X
<b>Software Management</b>		
Establish software license management policies	X	

<b>Thin Client</b>	<b>Government</b>	<b>Contractor</b>
Negotiate and procure software site or individual licenses that protect GSA right to use the software	X	
Track software assets (user, location, asset id, finances)		X
Maintain software product inventory as needed		X
Establish software migration/upgrade standards and policies	X	X
Develop detail procedures to ensure low-risk migration/upgrade		X
Test new releases of supported software to ensure conformance with GSA service level requirements		X
Install new releases of supported software on servers		X
Provide technical assistance during conversion as requested		X
<b>Monitoring and Reporting</b>		
Approve and document service levels and reporting cycles	X	
Measure and analyze performance relative to requirements		X
Develop improvement plans where appropriate	X	X
Implement improvement plans		X
Report on service level performance results		X
<b>Chargeback</b>		
Assign user account codes	X	
Maintain table for GSA account codes		X
Track utilization		X
Produce cost center invoices		X
Send invoices		X
Respond to GSA inquires		X

#### 6.4.5 Effort Estimate

Historically the effort to fulfill the requirements associated with Table 4.8 -2 Thin Client Services has been 7 contractor FTEs.

## 7. DELIVERABLES

The following deliverables are required in addition to the deliverable requirements identified in Section 19 of the General Cross-cutting PWS:

- 7.1. Deliverable #1: GSA Standard Image.** By the last day of each quarter, the Contractor shall submit an updated GSA Standard Image that is compliant with the requirements specified in section 6.2.4 “Image Management” of this sub-task and all applicable GSA guidance in Attachment 8.

**7.2. Deliverable #2: Monthly Systems Availability Report.** The Contractor shall provide monthly systems availability reports that present system availability data for the preceding month, and for the fiscal year to date - by user group and resource category. The Contractor shall meet with GSA monthly to review the issues regarding the work items associated with this sub-task and to review contractor recommended enhancements and/or modifications. The Contractor shall also provide data to meet GSA's information and analysis needs in areas including, but not limited to performance quality, production volumes, and adherence to sub-task requirements and standards, forecasting and trend projections. The Contractor's written progress reports shall include, as a minimum:

- 7.2.1. Summary of work completed including hours expended to accomplish work by each phase of this sub-task.
- 7.2.2. Problem report that lists all known issues.
- 7.2.3. List suggested enhancements and report on status of ongoing enhancements.
- 7.2.4. Status of ongoing site additions, closings, and modifications.
- 7.2.5. Status of ongoing activities associated with maintenance and operations.

**7.3. Deliverable #3: GEMS Technical Improvement Recommendation Reports.** Reports that present recommendations pertaining to implementations, configurations, operations, products, and technologies (including test results) for GEMS operation with particular regard to capacity planning.

**7.4. Deliverable #4: GNNI Technical Improvement Recommendation Reports.** Reports that present recommendations pertaining to implementations, configurations, operations, products, and technologies (including test results) for GNNI's groupware and collaboration environments.

**7.5. Deliverable Schedule.**

PARA	MILESTONE/ DELIVERABLE	PLANNED COMPLETION DATE
7.1	1 GSA Standard Image	Last day of each quarter
7.2	2 Monthly System Availability Reports	5th day of the month
7.3	3 GEMS Technical Improvement Recommendation Reports	By the 5 <sup>th</sup> working day of the quarter
7.4	4 GNNI Technical Improvement Recommendation Reports	By the 5 <sup>th</sup> working day of the quarter

**8. PLACE OF PERFORMANCE.**

The majority of the work contained in this sub-task, with the exception of client deployment services, will take place in the Washington DC Metro area, primarily at 1800 F Street NW, Washington, DC. Core client deployment services resources are expected to

emanate from the Washington DC Metro area but will of course travel to all GSA sites in order to maintain standardized client deployments across the enterprise.

**9. TRAVEL.**

This sub-task requires substantial travel within the continental United States as well as some OCONUS travel. Specific travel requirements are unknown at this time.

## **Appendix C: Sub-Task C - Consolidated Enterprise Help Desk**

### **1. BACKGROUND AND CURRENT ENVIRONMENT**

- 1.1.** The Government operates disparate help desks providing information technology infrastructure support services to its customers across the enterprise. There is a different help desk supporting each of the following major groups of customers:
  - 1.1.1. Central Office building – all persons, except the Office of Inspector General, Office of General Counsel and the Board of Contract Appeals
  - 1.1.2. Federal Acquisition Service – all persons comprising what was the Federal Supply Service and persons comprising some Regional Office locations of what was the Federal Technology Service.
  - 1.1.3. Federal Acquisition Service – all persons comprising headquarters office locations of what was the Federal Technology Service not covered above.
  - 1.1.4. Public Buildings Service – all persons comprising the Public Buildings Service separate by Region Office.
- 1.2.** Other help desks support the balance of customers. There are some instances where multiple help desks operate within the same location, but do not support the same customers. The numbers and locations of customers are itemized in Attachment 2.
- 1.3.** The help desks operate as separate entities. Each help desk follows its own set of procedures. There is not a standard enterprise resource management (ERM) framework. There are overlapping applications, multiple repositories of information and inconsistent reporting.
- 1.4.** The help desks support approximately 75% of customers through at least three unique Computer Associates Unicenter-based solutions. The majority of the other 25% of customers receive support through a best-in-breed approach featuring BMC Remedy with Proxy Remote Control and OnDemand WinINSTALL.
- 1.5.** The legacy product sets support the information technology infrastructure, applications and other program requirements. Application support personnel and program office personnel manage tickets within the legacy product sets.

### **2. OBJECTIVES**

The objectives of the Help Desk are to:

- 2.1.** Ensure availability of IT infrastructure resources to support the end user in meeting the GSA mission.
- 2.2.** Deploy a consolidated, enterprise help desk resulting in a reliable delivery of service and achieve a high level of customer satisfaction.
- 2.3.** Develop and deploy agency approved standard processes.
- 2.4.** Achieve cost savings through economies of scale and efficiencies resulting from

standardized processes.

- 2.5. Ensure complete documentation of processes and work requests.
- 2.6. Effectively maintain legacy product sets for infrastructure support through transition to the standardized ERM framework.
- 2.7. Effectively maintain and enhance the standardized ERM framework through the period of performance of the task order.
- 2.8. Provide for reliable 24 hour x 7 days a week help desk service via toll-free telephone number and e-mail for all users.
- 2.9. Provide for technical personnel who communicate clearly in English.

### **3. SCOPE**

The scope of this sub-task provides for operating a consolidated, enterprise help desk offering information technology infrastructure support. The consolidated, enterprise help desk is the single point of contact for all customers to report all incidents, submit all requests and register all complaints about the information technology infrastructure, applications and programs supported in the environment. The help desk supports simple requirements and escalates only complex requirements to the applicable local support personnel, personnel supporting another sub-task or a pre-approved, external support provider.

### **4. HELP DESK TASKS**

The following is a listing of tasks that may be required but is not limited to accomplish the objectives listed in Section 2 above:

- 4.1. Offer additional customer access to the consolidated, enterprise help desk such as web interface and instant messaging.
- 4.2. Document, investigate and diagnose each requirement. Determine impact and urgency to assign the priority (see Crosscutting PWS Section 17) for each incident, request and complaint.
- 4.3. Perform an initial assessment of all support requirements to identify those that the help desk is capable of resolving versus those requiring escalation to the applicable local support personnel or other support provider.
- 4.4. Resolve requirements via telephone and/or a combination of the standard ERM framework remote control feature.
- 4.5. Perform root cause analysis to assist with diagnosing and repairing problems and errors in the information technology infrastructure.
- 4.6. Perform predictive analysis to anticipate changes in call volume.
- 4.7. Provide call center support for applications and program office requirements. The Contractor shall route applicable incidents, requests and complaints to application support personnel or program office support personnel. The help desk shall follow up

with the customer to ensure the issue was resolved.

- 4.8.** Coordinate timely access to devices, systems and data (e.g., network, e-mail, network drives, applications, network printers/copiers, etc.) in accordance with standard operating procedures.
- 4.9.** Automate the processes and procedures necessary to allow help desk personnel to distribute automated installation packages, provide simple group administration, password resets, unlock network accounts, basic use of standard image software, and status of service availability and outages.
- 4.10.** Diagnose and repair incidents, requests and complaints over which they have the access and control to resolve.
- 4.11.** Diagnose and resolve incidents, requests and complaints with standard image applications. Educate customers on features of the standard image applications.

## **5. DELIVERABLES**

Deliverables for this subtask are identified in the Crosscutting PWS Section 19 – Communications and Deliverables.

## **6. PLACE OF PERFORMANCE**

The place of performance for this sub-task shall be the Contractor's facility (ies).

## **7. GOVERNMENT FURNISHED RESOURCES**

The Government will provide access to its network for the purpose of accessing systems for which the Contractor shall provide information technology infrastructure support. The Contractor shall abide by an interconnection agreement governing the relationship between the Contractor's information technology infrastructure and the Government's information technology infrastructure.

## **Appendix D: Sub-Task D - Local Support Services**

### **1. BACKGROUND**

GSA has disparate local support models providing information technology infrastructure support services to its customers across the enterprise. Onsite support needs to include servicing teleworkers. There is a different local support staff supporting each of the following major groups of customers:

- 1.1.** Central Office building – all persons except the Office of Inspector General, Office of General Counsel and the Board of Contract Appeals.
- 1.2.** Federal Acquisition Service – all persons comprising what was the Federal Supply Service and persons comprising some Regional Office locations of what was the Federal Technology Service.
- 1.3.** Federal Acquisition Service – all persons comprising headquarters office locations of what was the Federal Technology Service not covered above.
- 1.4.** Public Buildings Service – all persons comprising the Public Buildings Service separate by Region Office.
- 1.5.** Other local support staffs support the balance of customers. There are several instances where multiple local support staffs operate within the same location, but do not support the same customers. The numbers and locations of customers are itemized in Attachment 2.
- 1.6.** The local support staffs operate as separate entities. Each local support staff follows its own set of procedures. There is not one common set of procedures.

### **2. OBJECTIVES**

The following delineates the objectives of this task:

- 2.1.** Deploy a consistent level of IT support to GSA internal customers.
- 2.2.** Deploy a reliable quality of IT support to GSA internal customers.
- 2.3.** Ensure complete documentation of all local support activities in the standardized ERM framework.
- 2.4.** Achieve the most efficient operation possible through continuous process improvement.
- 2.5.** Achieve enterprise wide standard operating processes and procedures.
- 2.6.** Provide on site support personnel from 6:00 through 7:00 p.m. local time, Monday through Friday except federal holidays.
- 2.7.** Provide on site support to all locations including, but not limited to, Central Office, Headquarter Offices, Regional Offices and some mutually acceptable field offices

(see Attachment 2).

- 2.8. Provide local support after hours via on-call personnel.
- 2.9. Maintain accurate accountability and control of all government furnished equipment.
- 2.10. Provide responsive and reliable data communications circuit support.
- 2.11. Provide responsive support to Central Office for planned requirements that must occur on-site.

### 3. SCOPE

- 3.1 The scope of this sub-task includes providing local information technology infrastructure support on-site to customers located throughout the United States, Europe and Asia. Local support personnel diagnose and repair incidents, requests, and complaints with the information technology infrastructure. They also assist Central Office with actions, which must be accomplished on-site.
- 3.2 The on-site presence of local support assists with the infrastructure from the local LABN router down through and including all the hardware, software and cabling required in supporting the data, voice and video communications needs of the customers. Examples include communications support, local area network support and audio/video conferencing support.

### 4. SPECIFIC TECHNICAL REQUIREMENTS

The Contractor shall provide all administration and project management necessary to provide the customer with on-site, local support and Data Communications Circuit support.

- 4.1. **Local Support.** Local support activities generally include but are not limited to the following tasks:
  - 4.1.1. Accomplish information technology infrastructure support via telephone and remote control feature of the standardized ERM framework, on-site technical support personnel or dispatched support personnel to customers at the balance of field offices, places of business and other remote locations.
  - 4.1.2. Document incidents, requests and complaints in the standardized ERM framework. The help desk documents incidents, requests and complaints in the standardized ERM framework. Work accomplished by local support shall be documented in the standardized ERM framework. Local support personnel will follow procedures for referring helpdesk requests.
  - 4.1.3. Diagnose and repair incidents, requests and complaints received via the ticketing feature in the standardized ERM framework. Standard set of procedures in accordance with Government policy will be established as a deliverable for local support and helpdesk needs to be completed six months from award. The local support staff may need to consult with manufacturers, vendors and maintenance agreement holders to provide

support.

- 4.1.4. Provide moves, adds and changes (MACs) support. The Contractor performs moves, adds and changes on ten or fewer workstations. The client services subtask shall support moves, adds and changes of more than 10 workstations. The Contractor re-images workstations and performs technical refresh of workstations. This may or may not include migrating customer data from one machine to another workstation. The Contractor shall update asset management information.
- 4.1.5. Perform diagnosis and resolves incidents, requests and complaints with hardware, the operating system, standard image applications and other approved applications, and standard peripherals and telephones.
- 4.1.6. Provide audio, video and voice support available at the workstation. The Contractor assists with installing, maintaining and enhancing standard equipment and services including voice over internet protocol (VoIP) implementations.
- 4.1.7. Assist with installing, maintaining, consolidating, troubleshooting, repairing and enhancing local area networks. The Contractor assists with maintaining file and print servers and network traffic management devices including wireless access points.
- 4.1.8. Provide data backup and recovery assistance. The Contractor assists with backup and store media according to standard procedures and retention policy.
- 4.1.9. Provide facilities support. The Contractor installs, removes, maintains, consolidates and enhances fiber/twisted pair/coaxial cabling to support the enterprise infrastructure. The Contractor operates, maintains and enhances wiring closets and their contents including racks, power distribution units, cooling fans and uninterruptible power supplies (UPS). Approximately 2000 cable drops will be required on an annual basis.
- 4.1.10. Provide training support. The Contractor provides one-on-one training. The subject matter will be the use of any aspect of the information technology infrastructure, but typically, it will be on new service offerings, features of the workstation hardware, standard image software and approved application software, peripherals and telephones. The Contractor also supports classroom workstations.
- 4.1.11. Provide event support. The Contractor provides technical support to on-site and off-site conferences and meetings with 500 or fewer attendees. The Contractor transports government furnished equipment to the site or uses on-site equipment providing personnel with a valid driver license. The Contractor shall support internet and network access, workstations, peripherals, projectors, video and audio teleconferencing.

- 4.1.12. Provide inventory and supply management through existing Government systems. The Contractor maintains, dispenses and documents an inventory of government furnished equipment and supplies at each on-site location; for example cabling, associated supplies and UPS batteries, workstations and associated peripherals for temporary use, a supply of toner, storage media, etc.. The supply will be shared by customers at each location but will be attributed to specific customer organizations. The Contractor informs the Government of what needs to be ordered by when to ensure continued availability of supply.
- 4.1.13. Provides on-site assistance. These tasks may include the restarting of servers, switches or other devices; inputting commands into a system and relaying telephonically system responses; bios upgrades, etc.
- 4.1.14. Provide assistance to other subtasks with actions that must occur at the local on-site locations.

#### **4.2. Data Communications Circuits Support:**

Central Office, on behalf of the enterprise, manages approximately 500 data communications circuits to and among locations throughout the enterprise. The circuits include point-to-point (PTP) data circuits, Enterprise Digital Subscriber Line (eDSL) circuits over symmetrical DSL (SDSL) connections, asymmetric DSL (ADSL) circuit connections, cable circuits, wireless PTP/multipoint links, Enterprise Satellite (eSAT) terminal connectivity, Enterprise Integrated Services Digital Network (eISDN) circuits, frame relay circuits and asynchronous transfer mode (ATM) connections.

- 4.2.1. Currently data communications circuit support is available to customers in the Public Buildings Service (PBS) through the PBS Office of the Chief Information Officer and to the balance of customers across the enterprise through the GSA Office of the Chief Information Officer.
- 4.2.2. Data communication circuits shall be provided as GFE.
- 4.2.3. Data communication circuit support activities generally include but are not limited to the following tasks:
  - 4.2.3.1. Manage installation of data circuits to and among all locations (i.e., Central Office, Regional Offices, field offices and other locations) across the enterprise. Provide customer feedback on the installation of circuits. (i.e., usage, availability, projected installation date, etc.).
  - 4.2.3.2. Provide recommendations to improve program planning and business processes, including cost-benefit, risk and trade-off of implementing new technologies.

- 4.2.3.3. Provide recommendations and after analysis, provide planning, design, provisioning, modification and decommissioning of data circuits. Implement approved recommendations.
- 4.2.3.4. Provide technical and administrative support for various phases of the projects including circuit installation assistance and follow-on support as necessary in preparation for the next phase of technology deployment and implementation.
- 4.2.3.5. Perform monthly or quarterly, periodic processing and reconciliation of invoices from service providers for data circuits delivered. The Contractor shall automate this process to the greatest extent possible. It is preferred that this function be supported as part of the standardized ERM framework, if possible.
- 4.2.3.6. Perform financial analysis to include, but not limited to, Return on Investment (ROI) analysis, budget support, and cost monitoring activities.
- 4.2.3.7. Continuously research and evaluate new technology that could be exploited to better meet customer requirements, and support organizational goals and over-arching objectives.

## **5. DELIVERABLES**

Deliverables for this sub-task are identified in the Crosscutting PWS Section 19 – Communications and Deliverables.

## **6. PLACE OF PERFORMANCE**

The majority of the services under this sub-task shall be performed at the locations identified in Attachment 2 “Customer Locations and Counts” with the exception of the services under Section 4.2 Data Communications Circuits Support which shall be performed at the Washington D.C. Headquarters office.

## **7. TRAVEL**

Extensive travel to the field office locations and individual homes may be required in support of this sub-task. Specific travel requirements are unknown at this time.

## **Appendix E: Sub-Task E - Network Operations**

### **1. BACKGROUND**

Network Operations manages the agency-wide voice and data communications infrastructure. This includes the internetworking component of the enterprise infrastructure operations: the wide area network, local area backbone network, remote access, and voice and video services. Network Operations' services include:

- 1.1.** Wide Area Network Services
- 1.2.** Internetworking and Security Services
- 1.3.** Network Operations Center (NOC)
- 1.4.** Voice and Video Services
- 1.5.** Remote Access Services (RAS)

### **2. OBJECTIVE**

- 2.1.** The objective of this sub-task is to provide technical support services in the areas of network operations to include internetworking and security, local area networking, wide area networking, voice and video, and remote access.
- 2.2.** GSA OCIO must ensure voice and data communications services requirements are fulfilled in a technically competent and cost effective manner. This sub-task includes, but is not limited to, design and development, coordination, monitoring, requirements gathering, requirement analysis and validation, site surveys, deployment, patch management, security remediation, configuration management, lifecycle management, operational support, system support, and customer support.

### **3. SCOPE**

The Contractor shall provide the services enumerated in this sub-task to all users of the GSA enterprise infrastructure. The majority of the work contained in this sub-task will take place in the Washington DC Metro area but some work items may require personnel to be placed in other areas. Core administration and support resources are expected to emanate from the Washington DC Metro area but will of course travel to all GSA sites in order to support systems across the enterprise.

### **4. REQUIREMENTS**

#### **4.1. General Requirements**

- 4.1.1.** The Contractor shall provide monthly systems availability reports that present system availability data for the preceding month, and for the fiscal year to date. The Contractor shall meet with GSA monthly to review the issues regarding the work efforts associated with this sub-task and to review contractor recommended enhancements and/or modifications.
- 4.1.2.** This sub-task shall allow for staffing flexibility, quickly growing and/or

shrinking staff, in being able to respond to special projects such as PTT, emergencies, Executive mandates, etc.

- 4.1.3. The Contractor shall also provide data to meet GSA's information and analysis needs in areas including, but not limited to performance quality, production volumes, and adherence to sub-task requirements and standards, forecasting and trend projections.

## **4.2. Wide Area Network (WAN) Services**

### **4.2.1. Background**

The GSA Wide Area Network (WAN) is GSA's private wide area network that provides nationwide data communications and networking services for the agency. The WAN serves as the primary vehicle for interconnecting GSA's geographic locations and network users. The WAN is based on highly versatile multi-service CISCO MGX8850 switches, offering a combination of Frame Relay and ATM services, as well as high levels of network resiliency. The WAN interconnects 21 major locations nationwide. It uses AT&T and Sprint FTS2001 Public ATM Services, as well as local Public ATM Services, via DS3 and OC3 ATM facilities to provide a nationwide multi-path network topology that has redundancy and load balancing. Alternate routing capabilities are made possible due to a viable network architecture composed of primary and backup network paths using Permanent Virtual Circuits (PVCs) that range in bandwidth from 4 Mbps to 100 Mbps. The WAN's topology provides for a minimum of two network paths at each backbone node location within the continental United States. Network communications are supported by the WAN with either partially or fully meshed network architectures, as required by each network subscriber. The WAN architecture, itself, is meshed between backbone node locations and uses service providers for Layers 1 and 2 communication services. The WAN also supports network subscribers with dedicated point-to-point services that may range from 56 Kbps to T3, along with associated modems, data service units/communications service units (DSUs/CSUs) and other physical data communications components.

### **4.2.2. Objectives**

The objective is to provide technical support, maintenance and enhancement services for the GSA enterprise WAN.

### **4.2.3. Scope**

WAN equipment locations include GSA headquarters and 11 regional office buildings, and seven (7) field office locations and five (5) data centers. Headquarters and the regional offices located are in Washington, DC; Boston, MA; New York, NY; Philadelphia, PA; Atlanta, GA; Chicago, IL; Kansas City, MO; Fort Worth, TX; Denver, CO; San Francisco, CA; Auburn, WA.

The field offices are located in Arlington, VA; Vienna, VA; Springfield, VA; Anchorage, AK; Honolulu, HI; Los Angeles, CA, Hato Rey, and PR. The data centers are located in Chantilly, VA, Beltsville, MD., Eagan, MN, Salt Lake City, UT., and Phoenix, AZ.

4.2.4. Requirements

GSA OCIO requires contractor support to provide configuration, installation, documentation, and testing support for 25 Cisco MGX8850 switches nationwide. In addition, the Contractor shall configure, operate and maintain the WAN Network Management Systems (NMS), which consists of multiple Sun UNIX systems running the Solaris Operating System and Cisco WAN Manager. Tasks include design and configuration of the WAN to include all circuit, trunk, Permanent Virtual Circuit (PVC), Switched Virtual Circuit (SVC), and customer connections. Such connections include features for high-speed networking, switching, transmission, multimedia information exchange, and network layer protocols such as ATM and Frame Relay. Examples of typical work items associated with fulfilling these requirements are:

**Table 4.2.1. – 1 WAN Services Typical Work Item Examples**

<b>WAN Services</b>	<b>Government</b>	<b>Contractor</b>
<b>Operations and Administration</b>		
Coordinate configuration, testing, adjustment and implementation of WAN connections.	X	X
Collect and analyze network statistics for the various components of the WAN to determine and implement adjustments and improvements for optimized network performance and produce network statistics reports.		X
Provide high level troubleshooting and fault isolation and correction support for the WAN.	X	X
Save all WAN switch configuration files daily on the primary WAN NMS and backup to COOP Site.		X
Install and upgrade Cisco software in WAN switches as software releases become available.	X	X
Support the WAN Network Management Systems by installing and upgrading the NMS software as software releases become available, to include Solaris Operating System, Cisco WAN Manager, Cisco Statistics Manager/Collector, HP OpenView, HP Network Node Manager AND Informix Data Server.	X	X

<b>WAN Services</b>	<b>Government</b>	<b>Contractor</b>
Participate in the evaluation efforts associated with all WAN equipment. Evaluation of equipment includes establishing and conducting benchmark tests to determine if equipment is operating at specified performance levels. The Contractor shall convey the results of such evaluations.	X	X
Participate in the installation, de-installation and interconnection of WAN equipment as well as interconnection between WAN equipment and circuit/user interfaces.	X	X
Perform system interoperability testing endeavors	X	X
Perform Equipment Configuration and Implementation	X	X
Perform WAN Simulation/Modeling endeavors	X	X
Perform System and Network Optimization Tuning.	X	X
Perform Acceptance testing	X	X
The Contractor shall support the legacy product sets for infrastructure support until such time as GSA has migrated to a standardized ERM framework.		X
Document WAN components, designs and configurations, to include various customer connections, in electronic text and graphical form as appropriate.	X	X
Document Test Plans to include Acceptance and rejection criteria.	X	X
Develop and maintain Standard Operating Procedures (SOP). The SOP must contain at minimum: legacy product set for infrastructure support Operations, MGX8850 Switch Operations, Backup Configurations, Security Precautions, Contingency Plans, Quality Assurance (QA), and Configuration Requirements.		X
Provide professional graphical illustrations to depict present, proposed, and recommended solutions associated with evaluations, studies, analyses, etc.	X	X
Research and analyze development of packages and scripts to distribute software	X	X
Define requirements	X	
Identify possible product enhancement opportunities for improved performance and potential cost savings	X	X
Approve projects to implement product enhancement opportunity	X	
Identify possible product enhancement opportunities for improved performance and potential cost savings	X	X
Design, develop, operate, maintain and enhance (keep current) a test environment emulating the operating switches, workstations and servers	X	X

<b>WAN Services</b>	<b>Government</b>	<b>Contractor</b>
Interact with circuit, facility and customer equipment personnel to configure, test, adjust and implement WAN connections.	X	X
Establish software license management policies	X	
Establish supported software portfolio	X	
Negotiate and procure software site or individual licenses that protect GSA's right to use the software	X	
Track software assets (user, location, asset id, serial numbers, cost)	X	X
Maintain software product inventory as needed	X	X
Establish software migration/upgrade standards and policies	X	
Develop detail procedures to ensure low-risk migration/upgrade		X
Install new releases of supported software on servers	X	X

#### 4.2.5. Effort Estimate

Historically the effort to fulfill the requirements described in WAN Services requirements has been 2 contractor FTEs.

### 4.3. **Internetworking and Security Services**

#### 4.3.1. Background

Internetworking and Security Services manages the local area backbone network (LABN) and provides network security management for GSA infrastructure to include firewalls, intrusion detections and virus detection systems.

4.3.1.1. **Local Area Backbone Network.** The LABN component is based on a combination fiber-optic premise cabling system and Cisco router-based technology. LABN is located at all the Regional Office buildings and in the main data centers across the country. At each of the major GSA network nodes, LABN is composed of multiple routers and/or layer-3 switches to enable all LAN interconnections for that site via a collapsed backbone topology using fiber cabling. LABN provides connectivity among LANs in Regional Office buildings, GSA Secondary Networks, RAS, GEMS/GNNI, WEB services and the Internet. Inter-LABN communications are effected via the WAN and public tariffed services for internetworking, such as Asynchronous Transfer Mode (ATM), Frame Relay, and Dedicated Transmission Service (DTS). LABN is also the focal point for GSA's Internet access, which includes four T3 links to the ISP that are totally independent and provide for redundancy. The LABN core backbone network is made up of Cisco router models 7500, 7200

and Catalyst models 6500, 3500.

- 4.3.1.2. Secondary Network. The GSA Secondary Network consists of over 400 field office locations outside of the major LABN nodes. These sites are connected to the LABN nodes location via local and long haul HDLC 56K, T1, T3, fractional T1/T3, DSL, wireless, satellite, and site-to-site VPN. The Secondary Network uses Cisco router models 800, 2500, 2600, 2800, 3700, 3800, 4700 and Polycom xDSL routers to connect to LABN.
- 4.3.1.3. WebSense. The WebSense system contains fourteen enforcement points, geographically located around the country at each regional office, and one main data collection, management and reporting system located at central office. The enforcement point systems are running on Dell 2650's utilizing a Linux OS, and running the WebSense Employee Internet Management/Security Suite and Network Agent software. The Main data collection, management and reporting system run on a Windows Advanced 2000 Server, utilizing Microsoft's SQL Server 2000, WebSense Reporting, Explorer, Real-Time Analyzer, Database Engine, an Apache Web Server, and custom Microsoft Visual Basic Software.
- 4.3.1.4. Enterprise Network Security. Security services include 34 firewall servers of Checkpoint Firewall-1 clusters running Checkpoint Secure Platform on Dell 2550/2650 servers. These firewalls are deployed throughout GSA to protect GSA from external threats from the Internet as well as internal threats to sensitive data systems. There are over 30 Intrusion Detection Systems deployed in every major GSA node locations. These systems include ISS Real Secure, Network Flight Recorder (NFR), InterSpect, and NikSun. In addition to these IDS systems, there is also an internally developed security threat management application, code name "Weasel" that will identify, notify then shun the infected machine.
- 4.3.1.5. DNS. There are 32 DNS systems deployed in GSA. The GSA DNS system currently maintains one hundred sixty five (165) different domains, both forward and reverse domains, using a split-brain configuration separating GSA's internal and external domains. There are a total eighty-two (82) slave DNS servers comprising GSA's DNS System, internally (64) and externally (18), working as either slaves, slaves/forwarders, or hidden slaves servers. These systems are configured for fault-tolerant and high-availability using Cisco Content Services Switch (CSS)

and Multi Node Load Balancing (MNLB).

- 4.3.1.6. There are a total of twenty-one servers that are administered by the GSA DNS System Administrator running Send Mail and Bind, on 19 Postfix FreeBSD and Debian Linux servers, and two NT 4.0 servers.

#### 4.3.2. Objectives

GSA seeks technical assistance with the management and operational support for the GSA local area backbone network consisting of over 600 routers/switches and 170 security devices to ensure a high level of availability and application throughput.

#### 4.3.3. Scope

GSA provides internet and intranet connectivity as well as network security to over 400 locations nationwide and to some locations outside the continental U.S. such as Alaska, Hawaii and Puerto Rico, Europe and Asia.

#### 4.3.4. Requirements

The Contractor shall provide Inter-network and Security engineering support in the following area:

- 4.3.4.1. GSA internal backbone links via the GSA WAN.
- 4.3.4.2. GSA external links including Internet connections thru ISP and external network links such as another agency or company.
- 4.3.4.3. GSA Secondary Network links,
- 4.3.4.4. High-Speed Campus LAN architecture using links such as Fast and Gigabit Ethernet and dark fiber connections,
- 4.3.4.5. the configuration, management and administration of the LABN Network Management Systems,
- 4.3.4.6. the configuration, management, administration and operations of the GSA Employee Internet Management System (WebSense),
- 4.3.4.7. the configuration, management, administration and operations of the enterprise Network Security fabric environment,
- 4.3.4.8. the programming, administration, operations and maintenance of the Intrusion Detection and Audit systems,
- 4.3.4.9. The configuration, management, administration and operations of the DNS systems.
- 4.3.4.10. Work towards integration of all firewall, IDS and other network security instrumentation by providing communication avenues

for logs, which are sent to a centralized repository for collection and analysis.

4.3.4.11. Examples of typical work items associated with fulfilling these requirements are:

**Table 4.3 – 1 Internetworking And Security Services Typical Work Item Examples.**

<b>Internetworking and Security Services</b>	<b>Government</b>	<b>Contractor</b>
<b>Operations and Administration</b>		
Provide staff with knowledge and experience on Cisco router and switches models 7500, 7200, 6500, 3800, 3500, 2800, 2600, 800 and Polycom xDSL routers.		X
Responsible for analysis, design, testing, configuration, documentation and maintenance of all hardware/software components of LABN	X	X
Configure, administer and maintain seven SunSparc stations running Unix OS and have the skills and knowledge to manage CiscoWorks NMS, and HP OpenView.		X
Perform network analysis and capacity planning.	X	X
Support and manage protocol analyzers to diagnose network problems. These network tools will include Network Associates Sniffer, Network Instruments Observer Suites, NetQoS and CiscoWorks.		X
Research new technologies such as IPv6, VoIP and MPLS and evaluate impact on existing networks.	X	X
Install and upgrade Cisco IOS software in LABN routers and switches as new software releases or fixes become available.		X
Upgrade Cisco hardware equipment as needed according to the life cycle of the product or if the equipment is defective.		X
Design, configure, test, and troubleshoot all GSA internal and external WAN connections to include features for high-speed networking, switching, transmission, multimedia information exchange, and network layer protocols such as ATM and Frame Relay; DS-3, OC-3, T-3, T-1, DSL, and VPN between ISP and GSA WAN.	X	X
Analyze network statistics for the various components of the LABN to determine and implement adjustments and improvements for optimized network performance.		X
Configure, test, adjust and implement new LABN connections		X
Plan, design, configure, install, document, troubleshoot and test GSA's multi-homed Internet connections with its ISP	X	X

<b>Internetworking and Security Services</b>	<b>Government</b>	<b>Contractor</b>
Provide technical support in the management of routing protocols and technologies such as iBGP, eBGP, EIGRP, OSPF, SNMP, policy based routing, routing offset and distribute lists, IPSEC and GRE tunneling, VPN, NAT, and MPLS		X
Provide technical support in the management of large-scale inter-networks design, including the areas of implementation and troubleshooting techniques for IPv4, IPv6 and IPX protocols	X	X
Troubleshoot telecommunications systems and technologies including, but not limited to DS0 through DS3, DSL (eDSL, aDSL, iDSL, and sDSL), internetworking technologies (Ethernet, FDDI, and Multimode Fiber), and layers one through four of the OSI model		X
Provide technical support in the management of VLAN and VLAN trunking including 802.1Q and ISL, multicast, and spanning-tree		X
Provide technical expertise to operate and maintain multiple MRTG stations for monitoring those devices connected to the LABN.		X
Plan, design, test and implement rule based maintenance, transaction auditing, and log analysis of an enterprise-level firewall solution using Checkpoint Software's Firewall-1 software		X
Provide expertise in Checkpoint Firewall-1, VPN-1, SmartDefense, Floodgate, Interspect, High-Availability, Cluster XL, SecurePlatform, Hardened Linux 7.3, Centralized Logging, and Reporter Module		X
Provide technical support in the areas of programming, administration, operations and maintenance support for the deployed Intrusion Detection systems in the network. The Intrusion Detection systems are based on state-of-the-art technologies including ISS Real Secure, ISS Internet Scanner and Network Flight Recorder	X	X
Design and develop new features in Weasel to integrate it with IDS and IPS systems by using MySql Database and php programming for Web front-end	X	X
Network design, performance, security and trade-off considerations including throughput, latency, QoS, system availability, redundancy and fail-over such as HSRP	X	X
Administer, operate and maintain the GSA Domain Name Service (DNS) system in place.		X

<b>Internetworking and Security Services</b>	<b>Government</b>	<b>Contractor</b>
Provide technical expertise to operate and maintain multiple MRTG stations for monitoring those devices connected to the LABN.		X
Implement and document DNS changes, transaction auditing, automated system monitoring (CPU, Disk utilization, Service) and respond to alert notifications and support of MAPS RBL+ blackhole zonefiles.		X
Evaluate new emerging technologies to provide faster and cost effective networks to access information		X
Administer, operate and maintain the GSA Domain Name Service (DNS) system in place.		X
Design, test, implement, operate and maintain Domain Name System, BIND version 9.2.x on both FreeBSD and Debian Linux running on Dell 2650 behind a Cisco Content Switch (CSS 11500)		X
Verify the operational capabilities of all new equipment prior to deployment and coordinate all installations of such.		X

#### 4.3.5. Effort Estimate

Historically the effort to fulfill the requirements described in Table 4.3-1 Inter-networking and Security Requirements has been 12 contractor FTEs.

#### 4.4. **Network Operations Center (NOC/IISC).**

##### 4.4.1. Background

The Network Operations Center (NOC), also commonly referred to as the Information Infrastructure Support Center (IISC), assists the Government in monitoring, identifying, isolating, troubleshooting, correcting and documenting any/all problems within the GSA Information Infrastructure (GII), to include the WAN, LABN and Enterprise Security Infrastructure. The IISC also performs these functions for numerous secondary connections to the WAN or LABN from all GSA locations. Secondary connections may be point to point, frame relay, DSL, satellite and other technologies.

##### 4.4.2. Requirements

The Contractor shall staff the Network Operations Center (NOC), also referred to as the Information Infrastructure Support Center (IISC) to assist the Government in monitoring, identifying, isolating, troubleshooting, correcting and documenting any/all problems within the GSA Information Infrastructure (GII) to include the Wide Area Backbone Network (WAN), Local Area Backbone Network (LABN), Enterprise Firewalls and Remote Access Service (RAS)

- 4.4.2.1. The majority of problems that occur on the GII include but are not limited to circuit outages, system crashes, and power outages. These problems as well as all others, shall be logged by the NOC into the legacy ticket processing product [currently this is Remedy Action Request System (RARS)], with the date, time, affected system information and sequence of events leading up to the correction of the problem, so if needed senior technical support staff can conduct further analysis. The legacy ticket processing product, RARS, is used by government and contractor personnel to aid in workflow and problem resolution to support the various components of the information infrastructure.
- 4.4.2.2 Examples of typical work items associated with fulfilling these requirements are:

**Table 4.4 – 1 Network Operations Center Typical Work Item Examples**

<b>Network Operations Center</b>	<b>Government</b>	<b>Contractor</b>
<b>Operations and Administration</b>		
Keep all WAN, LABN, Enterprise Firewall, and RAS systems within the GSA Information Infrastructure (GII) up and running. This may include, scheduling system or power outages, scheduling maintenance, and notifying the Project Manager (PM) and/or his subordinate(s) of any major events occurring within the GII.		X
Properly staff the NOC/IISC stations, which must provide a comprehensive, end-to-end view of activity throughout the WAN, LABN, Enterprise Firewall, and RAS. Provide that all technical personnel be required, but not limited, to configuring, installing, supporting, managing, and administering the WAN, LABN, Enterprise Firewall, RAS within the NOC/IISC and be qualified to provide high level of support on all network communications components including but not limited to the following: Cisco router models 7500, 7200, 3600, 2600, 2500 and 800; Cisco Catalyst series 6500 and 2900; modems; network control consoles; Data Service Units (56K, Fractional T1, T1, Frame Relay); Efficient xDSL Routers and Polycom xDSL Routers; and Cisco router models AS5200, 53X0, 800 and 700 series routers.		X
Maintain a real-time on-line operations log in the standardized ERM framework of all WAN, LABN, Enterprise Firewall, and RAS network calls, events and resolutions that rectify the specific situation.		X

<b>Network Operations Center</b>	<b>Government</b>	<b>Contractor</b>
Monitor multiple RAS Cisco Secure Access Control Servers (ACS) and their PRI connections to different vendors throughout the GII by using NMS CiscoWorks and What's Up Gold in order to maintain operations.		X
Optimize performance, perform system station back-ups on a weekly basis, and recover and configure and connect hardware.		X
Provide the technical expertise to review and validate all telecommunications circuits and formulate recommendations for retention, cancellation or transfer of responsibility.		X
Maintain a real-time database of the installed equipment detailing: equipment descriptions, serial numbers, quantities, locations, maintenance levels, circuit IDs and inventories, and Point-of-Contacts as well as tracking all network router installations to include equipment descriptions, serial numbers, quantities, locations, maintenance level, and circuit inventories.		X
Notify individuals responsible for the affected systems and identify, analyze and troubleshoot the problem by performing diagnostics to isolate the faults, contacting and coordinating with service providers (if necessary for repair), contacting and coordinating GSA Regional personnel (if necessary), and logging the complete detailed event in the standardized ERM framework for future analysis by the senior technical support staff, if needed, when alerted to a problem or an alarm condition occurs.		X
Perform network management functions. Network management involves activities related to the real-time monitoring of the WAN and LABN using Cisco WAN Manager and other network management sub-systems. Some of the activities include:		X
Monitoring for the occurrence of Network Exceptions (Fault Dockets) reported via alarm systems on a Computer Video Screen;		X
Responding to reported Network Exceptions (Fault Dockets) in a timely manner (depending on the severity of the exception, may require making telephone calls; using network monitoring utilities to investigate and perform remediation of the reported problem; or referring the problem to a senior engineer in an attempt to rectify the abnormal network situation);		X
Closing out Fault Docket after problem is resolved; and		X

Network Operations Center	Government	Contractor
Use the Wide Area Network (WAN) Network Management Systems available to have a real time measurement of the health of the WAN.		X

4.4.3. Effort Estimate

Historically the effort to fulfill the requirements described in Table 4.4 – 1 Network Operations Center Requirements has been 12 contractor FTEs.

4.4.4. Hours

To perform this service, the Contractor shall provide coverage to operate the IISC twenty-four (24) hours per day, five (5) days per week.

4.4.4.1. The Contractor shall provide on-call pager/cell phone weekend support coverage from Saturday 12:01am to Sunday 11:59pm EST, including but, not limited to all government Holidays, inclement weather and all other government related closings that could possibly exist in the Washington, DC area..

**4.5. Voice And Video Services**

4.5.1. Background

The GSA Office of the CIO manages and provides infrastructure to include voice landline communications, voice cellular services, Voice over Internet Protocol (VoIP), as well as video communications infrastructure. Currently GSA is using a decentralized multi-faceted approach to Voice and Video technologies and services. GSA’s vision is to evolve to a more efficient model for Voice and Video technologies and services.

4.5.2. Objective

To provide the Government with professional and technical management, operations and on-going maintenance of the GSA Voice and Video infrastructure as well as support in the accomplishment of GSA’s Voice and Video services vision.

4.5.3. Scope

GSA’s Voice and Video Services infrastructure. Systems are located at GSA headquarters and 11 regional office locations. Headquarters and the regional offices locations include Washington, DC; Boston, MA; New York, NY; Philadelphia, PA; Atlanta, GA; Chicago, IL; Kansas City, MO; Fort Worth, TX; Denver, CO; San Francisco, CA, and Auburn, WA, Asia and Europe. The Contractor shall assist the Government in standardizing all such resources and deploying and maintaining a centrally managed enterprise Voice and

Video Services infrastructure.

4.5.4. Requirements

- 4.5.4.1. The Contractor shall provide management, maintenance and on-going operation support for the GSA voice, data and video infrastructure, which includes all analog, digital, VoIP and wireless services, software, voice mail systems and related equipment.
- 4.5.4.2. The Contractor shall plan and manage the migration of any existing stand alone regional VoIP implementations, so that they are incorporated into the GSA Enterprise VoIP architecture. The GSA Enterprise VoIP Architecture is a single cluster architecture, with all eleven regional offices configured with a single centrally controlled configuration and architecture.
- 4.5.4.3. The Contractor shall design, implement and manage the E911 solution, to ensure that there is failover and redundancy built into the configuration. The Contractor shall ensure that all E911 services are functional and operational.
- 4.5.4.4. The Contractor shall design, implement and manage the VoIP system to fully integrate with GSA's Lotus Notes Email Environment as well as GSA's Active Directory Environment. The Contractor shall ensure that the VoIP system is interoperable with any existing Contact Center Systems.
- 4.5.4.5. The Contractor shall manage all internal agency-wide voice communications systems components of the GSA information infrastructure to include Voice Land Line communications, Voice Cellular Services, Voice over Internet Protocol (VoIP), and other related technologies including Satellite, Data, Packet, Radio, wireless, etc., supporting GSA missions including centralized program management, best practices analyses, customer services standards, continuous process improvement and regional support coordination.
- 4.5.4.6. The Contractor shall design, develop, implement, manage and maintain GSA internal Telecommunication networks and Video systems.
- 4.5.4.7. The Contractor shall ensure coordination and/or compliance with all existing contracts, guidelines and regulations pertaining to telecommunications management and operations in the Federal Government.

- 4.5.4.8. The Contractor shall provide management and operation support of GSA's Video communications infrastructure, including analog videoconferencing, digital IP videoconferencing, Video conference rooms, Desktop Video and Mobile video services and multicasting
- 4.5.4.9. The Contractor shall analyze and determine solutions for requirements of all new Telecommunications and Video services and programs.
- 4.5.4.10. The Contractor shall manage, operate, and maintain all internal digital voice mail systems.
- 4.5.4.11. The Contractor shall establish and maintain automated systems for the ordering and tracking of telecommunications services and devices including serial numbers, circuit numbers and phone numbers to manage the identification, verification, and certification of telecommunications invoices.
- 4.5.4.12. The Contractor shall manage an inventory of new/used/defective/obsolete equipment and implement, re-issue or excess as appropriate.
- 4.5.4.13. The Contractor shall troubleshoot Telecommunications and Video problems and take appropriate actions to repair and/or restore services as necessary.
- 4.5.4.14. The Contractor shall maintain constant vigilance on emerging voice and video technologies and provide recommendations on the proper application of such technology to the GSA environment.
- 4.5.4.15. The Contractor shall design and implement a Voice and Video Test Laboratory for the purpose of providing a demonstration and testing environment for testing new products. There exists a fully equipped (hardware and software) laboratory at GSA Headquarters. However, this may change in the future to a government facility in one of the Regions.

#### **4.6. Remote Access Services (RAS)**

##### **4.6.1. Background**

- 4.6.1.1. GSA's Remote Access Services (RAS) permits GSA associates and authorized contractors to gain access to GSA's systems anytime and from anywhere. The RAS solution has been structured to handle both the remote access and remote control requirements. Cisco's AS5x00 Universal Access Server platforms have been

deployed in each of the 11 GSA Regional Office Buildings, Central Office, Crystal City (Virginia), Hawaii, Alaska, Puerto Rico and Los Angeles. The RAS infrastructure provides a point-to-point protocol transport for analog dial-up and Integrated Services Digital Services (ISDN) connections along with Enterprise Digital Services (eDSL) and Virtual Private Network (VPN) connectivity. Security and centralized management of existing accounts and connections are provided using Cisco's Access Control Servers (ACS) CiscoSecure Servers, which are located at GSA's Central Office and Kansas City locations with backup servers located in Fort Worth and Atlanta. The RAS Team and the NOC assist the local support in RAS user account administration, and proactively monitor the network for potential problems

- 4.6.1.2. The RAS CORE Dial Network Infrastructure is comprised of 13 Cisco AS5350 Router's located nationwide in GSA Region's 1 – 10, NCR, Central Office and Puerto Rico. The regional Cisco AS5350's are configured with varies site dependant data Primary Rate Interface (PRI) configurations. The RAS regional Cisco AS5350's PRI can support up to 1000 simultaneous dialup sessions nationwide. The RAS CORE network provides dialup connectivity for over 12,000 GSA employees and internal contractors.
- 4.6.1.3. The VPN Infrastructure is comprised of 10 Nokia IP530/IP560 clustered appliances, located in 3 GSA regional locations (CO, R6 and R9). The VPN Infrastructure is designed using the Nokia IP530/IP560 Appliances that operate on the Checkpoint VPN-1 NG/NGX Secure Platform (SPLAT) Software. The VPN Nokia Appliance and Checkpoint software provide IP Security (IPSec) Split-Tunneling technology to over 6000 VPN GSA employees, internal and external contractors. The VPN IPSec end-user connection is established via the Checkpoint "Secure Client" licensed software. The IPSec VPN also supports VPN Site to Site; the VPN supports over 20 Site to Site locations regionally.
- 4.6.1.4. The RAS eDSL System Support is designed to provide eDSL end user information to GSA employees who choose to subscribe to GSA's direct high speed network access. GSA's eDSL offers connectivity from Covad Communications and managing partner Comtech LLC and GSA's LABN Core Routers to provide direct high-speed access for residential GSA customers. The RAS Web Page is also utilized to provide eDSL end- user requests, qualification checks, documentation, download, client install,

FAQ's and eDSL policy information.

4.6.2. Objective

To enable access to the GSA information infrastructure from anywhere at any time.

4.6.3. Scope

The RAS Management Systems are located in Central Office with backups in Region 6 Kansas City.

4.6.4. Requirements

GSA seeks full enterprise-wide operational support for its remote access infrastructure including dial-up, VPN, wireless, and other technologies. Examples of typical work items associated with fulfilling these requirements are:

**Table 4.6 -1 RAS Typical Work Item Examples**

<b>Roles and Responsibilities</b>	<b>Government</b>	<b>Contractor</b>
<b>Operations and Administration</b>		
Knowledge of Remote Access and Remote Control technologies, specifically pertaining to the Cisco AS5200, 5300, 800, and 700 series routers.		<b>X</b>
Perform monitoring of the GSA RAS infrastructure from a CiscoWorks management station.		<b>X</b>
Log all trouble calls into the standardized ERM framework. The Contractor shall provide support for maintaining and updating the User Client database.		<b>X</b>
Monitor, operate, maintain and troubleshoot, agency-wide day-to-day RAS and Remote Control technologies to include, RAS Dial-up, Integrated Services Digital Network (ISDN), Virtual Private Network (VPN), and Enterprise Digital Services Network (eDSL) connectivity.		<b>X</b>
Support on all RAS network communications components including but not limited to, Cisco router models 700, 800 and AS53x0's.		<b>X</b>
Perform monitoring of multiple RAS Cisco Secure Access Control Servers (ACS) and their PRI connections to different vendors throughout the GII by using NMS CiscoWorks and What's Up Gold in order to maintain operations.		<b>X</b>

<b>Roles and Responsibilities</b>	<b>Government</b>	<b>Contractor</b>
Provide a higher tier level of expertise in RAS support to the Regional Local Support Staffs, which includes but not limited to administrating and troubleshooting authentication and connectivity issues with RAS Dial-up, ISDN, VPN, or eDSL.	<b>X</b>	<b>X</b>
Setup and install Checkpoint "Secure Client" and its functions.	<b>X</b>	<b>X</b>
Configure and monitor VPN systems using Smartview Tracker, Status and Dashboard to maintain operations and support LAN Administrators to troubleshoot VPN user accounts and connectivity issues with logging into the network.	<b>X</b>	<b>X</b>
Monitor and troubleshoot the multiple DSL Backhaul connections throughout the GII. The Contractor shall assist in the setup, install and troubleshooting process of the eDSL end-user Clients (PPPoE Internet Client) with the Local Support Staffs, if necessary.	<b>X</b>	<b>X</b>
Maintain a RAS test lab environment and a RAS test Core environment.	<b>X</b>	<b>X</b>
Provide and maintain logical schematics of the RAS Cisco AS5350 Router network connectivity.		<b>X</b>
Provide installation and troubleshooting of dedicated and dial circuits including ISDN, Analog, and Data Primary Rate Interfaces (PRI) with the local phone companies.		<b>X</b>
Perform administration, operations and monitoring of the GSA RAS CORE Cisco AS5350 routers using Cisco Works and Cisco Secure software tools.		<b>X</b>
Log all trouble calls into the standardized ERM framework.		<b>X</b>
Provide qualified engineering support to assist in the planning, design, configuration, installation, maintenance, monitoring, security, troubleshooting, project management, documentation, testing and emerging technologies support for the VPN networking components. .		<b>X</b>
Coordinate with the IO staff to make all connections and configurations necessary for all components of the VPN Infrastructure.		<b>X</b>
Provide engineering support for a RAS SSL VPN solution, which is currently being designed to offer to all GSA employees, internal and external contractors.		<b>X</b>
Maintain a test VPN Lab environment.		<b>X</b>
Provide and maintain logical schematics of the VPN network connectivity.		<b>X</b>
Provide installation and troubleshooting of the VPN Infrastructure.		<b>X</b>

<b>Roles and Responsibilities</b>	<b>Government</b>	<b>Contractor</b>
Document all VPN installations with inventory documents listing serial numbers of all equipment, IP assignments, location and contacts.		<b>X</b>
Perform administration, operations and monitoring of the VPN network using Checkpoint VPN-1 Manager System, Smart Dashboard and Cisco Works.		<b>X</b>
Provide qualified engineering support to assist in the planning, design, configuration, installation, maintenance, troubleshooting, monitoring, security, project management, documentation, testing and emerging technologies support of GSA's RAS eDSL System Support.		<b>X</b>
Provide qualified engineering support to implement and troubleshoot eDSL connectivity.		<b>X</b>
Assist GSA IOS staff in the design, implementation, and ongoing support of GSA's eDSL system.		<b>X</b>
Support users with the setup and configuration of remote eDSL installations.		<b>X</b>
Provide qualified engineering support to assist in the planning, design, configuration, installation, maintenance, troubleshooting, monitoring, security, project management, documentation, testing and emerging technologies support of GSA's RAS Management System components		<b>X</b>
Provide design, programming, installation, administration, maintenance, troubleshooting, monitoring, security, project management, documentation, testing and emerging technologies support for the RAS Management and Reporting System components		<b>X</b>
Monitor the RAS system components 24 x 7 by using appropriate monitoring and alerting software such as SQL, internet web servers, logging tools, Cisco Works, Sitescope, MRTG, Mobile Automation, and Cisco ACS servers. CPU load, available disk space, as well as downed system services must be tracked and alerts sent out to appropriate staff via email or pager when configured thresholds are exceeded.		<b>X</b>
Have a solid Security systems understanding and specific knowledge of industry best practices, government regulations requiring the installations and configuration of network components including, but not limited to Cisco, SANS, NIST, GAO and OMB		<b>X</b>

Roles and Responsibilities	Government	Contractor
Assist GSA in evaluating new technologies to provide faster and cost effective networks to access information. Some of the new initiatives the Contractor shall be reviewing include xDSL technologies, Public Key Infrastructure (PKI), Voice-over-IP (VoIP), IPv6, Video Conferencing, SSL VPN, and Endpoint Security solutions.		<b>X</b>

4.6.5. Place of Performance

The place of performance shall be government offices at GSA, 1800 F Street, Washington, D.C.

4.6.6. Hours

These services will normally be performed during the core work hours of 7:00 AM to 7:00 PM, Monday through Friday. However, the Contractor may be required to work outside the core work hours in response to emergency requirements. Also, occasional overtime support and on-call coverage may be required (this includes the weekend, early morning hours, late evening hours, and Federal holidays).

4.6.7. Effort Estimate

Historically the effort to fulfill the requirements described in Table 4.6 -1 RAS Requirements has been 10 FTEs.

**5. DELIVERABLES**

Deliverables for this subtask are identified in the Crosscutting PWS Section 19 – Communications and Deliverables.

**6. TRAVEL.**

This sub-task requires substantial travel within the continental United States as well as some OCONUS travel. Specific travel requirements are unknown at this time.

## Appendix F: Acronym Dictionary

Acronym	Word/Phrase	Definition
ACD	automated call distribution	Automatic Call Distribution: takes incoming calls and evenly distributes them to service agents, providing relevant caller information.
aDSL	asymmetric DSL	ADSL divides up the available frequencies in a line on the assumption that most Internet users look at, or download, much more information than they send, or upload. Under this assumption, if the connection speed from the Internet to the user is three to four times faster than the connection from the user back to the Internet, then the user will see the most benefit (most of the time).
ARS	Action Request System	Service Process Management system produced by BMC Software. See <a href="http://www.bmc.com">www.bmc.com</a>
ATM	Asynchronous Transfer Mode	A cell relay network protocol which encodes data traffic into small fixed-sized (53 byte; 48 bytes of data and 5 bytes of header information) cells instead of variable sized <i>packets</i> (sometimes known as <i>frames</i> ) as in packet-switched networks (such as the Internet Protocol or Ethernet). It is a connection-oriented technology, in which a connection is established between the two endpoints before the actual data exchange begins.
BEAS	Blackberry Enterprise Access Servers	A wireless platform solution that allows Blackberry users to interface with IBM® Lotus® Domino® messaging and collaboration applications.
BIND	Berkeley Internet Name Domain	The Internet and almost all local networks depend upon a working and reliable <i>Domain Name Service (DNS)</i> , which is used to resolve names of systems into IP addresses and vice versa. In order to facilitate DNS on a network, a nameserver is required to translate these names into the IP addresses necessary to make the connection. In addition, a nameserver can translate IP addresses back into a system's name, commonly called a reverse lookup
CA	Computer Associates	A computer hardware, software and services company. <a href="http://www.computerassociates.com">www.computerassociates.com</a>
CD	Compact Disc	An optical disc used to store digital data, originally developed for storing digital audio.

Acronym	Word/Phrase	Definition
CLIN	Contract Line Item Number	Provides a structure for the evaluation of a portion (or in some cases all) of the submitted proposal or quotation.
COOP	Continuity of Operations Plan	Continuity of Operations Plans refer to preparations and institutions maintained by the U.S. Government that provide for governmental survival in the case of catastrophic events.
CSS	Cisco Content Services Switch	see <a href="http://www.cisco.com">www.cisco.com</a>
CSU	Channel Service Unit	The CSU terminates the external line at the customer's premises. It also provides diagnostics and allows for remote testing
DBA	Database Administrator	A person who is responsible for the environmental aspects of a database
DCE	distributed computing environment	DCE supplies a framework and toolkit for developing client/server applications. The framework includes a remote procedure call (RPC) mechanism known as DCE/RPC, a naming (directory) service, a time service, an authentication service, an authorization service and a distributed file system (DFS) known as DCE/DFS.
DHCP	Dynamic Host Configuration Protocol	A protocol that provides a means to dynamically allocate IP addresses to computers on a local area network. The system administrator assigns a range of IP addresses to DHCP and each client computer on the LAN has its TCP/IP software configured to request an IP address from the DHCP server. The request and grant process uses a lease concept with a controllable time period.
DNS	Domain Name System	The name resolution system that lets users locate computers on a Unix network or the Internet (TCP/IP network) by domain name. The DNS server maintains a database of domain names (host names) and their corresponding IP addresses. In this hypothetical example, if <b>www.mycompany.com</b> were presented to a DNS server, the IP address <b>204.0.8.51</b> would be returned. DNS has replaced the manual task of updating HOSTS files in an in house Unix network, and of course, it would be impossible to do this manually for the global Internet.
DOA	Date of Award	Date of Award

Acronym	Word/Phrase	Definition
DSL	Digital Subscriber Line	This technology uses the copper pair wiring that exists in almost every home and office. Special hardware attached to both the user and switch ends of line allows data transmission over the wires at speeds normally in the range of 1.5 to 5.0 Megabytes per second (Mbps).
DSU	Digital (or Data) Service Unit	The DSU does the actual transmission and receiving of the signal and provides buffering and flow control for the T1 interface.
DTS	Dedicated Transmission Service	High speed (usually T-1 or greater) dedicated transmission service between two locations
DVD	Digital Video Disc	A disk coated with plastic that can store digital data as tiny pits etched in the surface; is read with a laser that scans the surface
EAC	Election Assistance Commission	The U.S. Election Assistance Commission (EAC) was established by the Help America Vote Act of 2002 (HAVA). Central to its role, the Commission serves as a national clearinghouse and resource for information and review of procedures with respect to the administration of Federal elections.
eBGP	External Border Gateway Protocol	The core routing protocol of the Internet. It works by maintaining a table of IP networks or 'prefixes' which designate network reach ability between autonomous systems (AS). It is described as a path vector protocol. BGP does not use traditional IGP metrics, but makes routing decisions based on path, network policies and/or rule sets. As of January 2006, the current version of BGP, version 4, is codified in RFC 4271.
eDSL	Enterprise Digital Subscriber Line	DSL service provided throughout an enterprise extending internationally if required.
EIGRP	Enhanced Interior Gateway Routing Protocol	A proprietary routing protocol from Cisco
eISDN	Enterprise Integrated Services Digital Network	ISDN implementation throughout an enterprise.
EIT	Electronic and Information Technology	Defined at <a href="http://www.access-board.gov/508.htm">http://www.access-board.gov/508.htm</a>
ERM	Enterprise Resource Management	Defined in Cross Cutting Section 15
eSAT	Enterprise Satellite	Terminal connectivity solution

Acronym	Word/Phrase	Definition
EVMS	Earned Value Management System	A structured system for evaluating a project's progress in terms of the accrued value of the work accomplished with respect to the project's budget and schedule.
FAS	Federal Acquisition Service	See <a href="http://www.gsa.gov">www.gsa.gov</a>
FDDI	Fiber Distributed Data Interface	FDDI was an ANSI standard token passing network that transmitted 100 Mbps over optical fiber up to 10 kilometers. It included its own network management system and could optionally run over copper wire (CDDI) with distance limitations. FDDI II added circuit-switched service to this normally packet-switched technology in order to support isochronous traffic such as real time voice and video.
FIPS	Federal Information Processing Standards	A series of publications issued by the U.S. National Institute of Standards and Technology (NIST) that specifies information security guidelines for federal government departments and agencies. For more information, visit <a href="http://www.itl.nist.gov/fipspubs/index.htm">www.itl.nist.gov/fipspubs/index.htm</a>
FSS	Federal Supply Service	GSA Federal Supply Service, see <a href="http://www.gsa.gov">www.gsa.gov</a>
FTR	Federal Travel Regulation	Statutory requirements and Executive branch policies for travel by federal civilian employees and others authorized to travel at government expense. See <a href="http://www.gsa.gov">www.gsa.gov</a>
FTS	Federal Technology Services	GSA Federal Technology Services, see <a href="http://www.gsa.gov">www.gsa.gov</a>
GAO	Government Accountability Office	See <a href="http://www.gao.gov">www.gao.gov</a>
GEMS	GSA's Enterprise Messaging Services	The IBM Lotus Sametime messaging service implemented within GSA
GFE	Government Furnished Equipment	Those physical items supplied to a vendor to assist in the fulfillment of contractual requirements.
GII	GSA Information Infrastructure	Describes the installed heterogeneous base of hardware and software within GSA.
GNNI	GSA National Notes Infrastructure	Refers to the Lotus Notes hardware and software infrastructure installed throughout GSA.

Acronym	Word/Phrase	Definition
GRE	Generic Routing Encapsulation	A tunneling protocol designed for encapsulation of arbitrary kinds of network layer packets inside arbitrary kinds of network layer packets. The original packet is the payload for the final packet. For example, tunnel servers, which encrypt can use GRE to tunnel through the Internet for secure virtual private networks.
GSA	General Services Administration	See <a href="http://www.gsa.gov">www.gsa.gov</a>
GSA CO	GSA Contracting Officer	Defined in Cross Cutting Section 4
GSA COR	GSA Contracting Officer's Representative	Defined in Cross Cutting Section 4
GSA COTR	GSA Contracting Officer's Technical Representative	Defined in Cross Cutting Section 4
GSA PM	GSA Program Manager	Defined in Cross Cutting Section 4
HSPD 12	Homeland Security Presidential Directive 12	Policy for a Common Identification Standard for Federal Employees and Contractors. See <a href="http://csrc.nist.gov/policies/Presidential-Directive-Hspd-12.html">csrc.nist.gov/policies/Presidential-Directive-Hspd-12.html</a>
HSRP	Hot Standby Router Protocol	A protocol from Cisco for switching to a backup router in the event of failure
iBGP	IP Border Gateway Protocol	The iBGP Multipath Load Sharing feature enables the BGP speaking router to select multiple iBGP paths as the best paths to a destination.
IDS	Intrusion Detection System	Software that detects an attack on a network or computer system.
iDSL	ISDN Digital Subscriber Line	Transmits data digitally (rather than analog) on a regular twisted pair copper telephone line, across existing ISDN lines, at a rate of 144 kbit/s, slightly higher than a bonded dual channel ISDN connection at 128kbit/s.
IDSN	Integrated Services Digital Network	A type of circuit switched telephone network system, designed to allow digital transmission of voice and data over ordinary telephone copper wires, resulting in better quality and higher speeds than available with analog systems.
IISC	Information Infrastructure Support Center	GSA Information Infrastructure Support Center

Acronym	Word/Phrase	Definition
IP	Internet Protocol	A data-oriented protocol used for communicating data across a packet-switched network.
IPSEC	IP security	A standardized framework for securing Internet Protocol (IP) communications by encrypting and/or authenticating each IP packet in a data stream.
IPv4	Internet Protocol Version 4	The fourth iteration of the Internet Protocol (IP) and it is the first version of the protocol to be widely deployed. IPv4 is the dominant network layer protocol on the internet.
IPv6	Internet Protocol Version 6	An improvement over the IPv4 specification increasing the number of addresses available for networked devices,
IPX	IPX	A network protocol stack used by Novell Netware
ISL	Inter-Switch Link	A proprietary Cisco protocol
ISOC	Infrastructure Systems Operations Center	GSA's Infrastructure Systems Operations Center
ISP	Internet Service Provider	Is a business or organization that sells to consumers' access to the Internet and related services.
ISS	Internet Security Systems	Internet Security Systems, Inc. See <a href="http://www.iss.net">http://www.iss.net</a>
ISSM	Information System Security Manger	Defined in "Standard Operating Procedure for GSA HSPD-12 Personnel Security Process"
ISSO	Information System Security Officer	Defined in "Standard Operating Procedure for GSA HSPD-12 Personnel Security Process"
IT	Information Technology	Is concerned with the use of technology in managing and processing information.
ITAPC	GSA Information Technology Architectural Planning Committee	GSA Information Technology Architectural Planning Committee
ITIL	Information Technology Infrastructure Library	A framework of best practice approaches intended to facilitate the delivery of high quality information technology (IT) services. ITIL outlines an extensive set of management procedures that are intended to support businesses in achieving both quality and value for money in IT operations. These procedures are supplier independent and have been developed to provide guidance across the breadth of IT infrastructure, development, and operations.
ITSS	IT Solution Shop	See: <a href="http://itss.gsa.gov">itss.gsa.gov</a>

Acronym	Word/Phrase	Definition
IVR	Interactive Voice Response	An automated telephone information system that speaks to the caller with a combination of fixed voice menus and data extracted from databases in realtime.
LABN	Local Area Backbone Network	Connects nodes of the local area network.
LAN	Local Area Network	A computer network covering a local area, like a home, office, or group of buildings
LDAP	Lightweight Directory Access Protocol	A networking protocol for querying and modifying directory services running over TCP/IP.
MAC	Moves, adds, and changes	Moves, adds, and changes
MNLB	Multi Node Load Balancing	A technique to spread data traffic between many backbone nodes or other resources in order to get optimal resource utilization and data transmission time.
MPLS	MultiProtocol Label Switching	A standard from the IETF for including routing information in the packets of an IP network. MPLS is used to ensure that all packets in a particular flow take the same route over a backbone. Deployed by many service providers, MPLS can deliver the quality of service (QoS) required to support realtime voice and video as well as service level agreements (SLAs) that guarantee bandwidth.
MRTG	Multi Router Traffic Grapher	Software for monitoring the traffic load on network links. It shows traffic load on a network over time in graphical form.
NACI	National Agency Check with written Inquiries	Low risk security check see <a href="http://www.dhs.gov">www.dhs.gov</a>
NACIC	National Agency Check with written Inquiries and Credit	Low risk security check see <a href="http://www.dhs.gov">www.dhs.gov</a>
NAS	Network-attached storage	The name given to dedicated data storage technology that can be connected directly to a computer network to provide centralized data access and storage to heterogeneous network clients.
NAT	Network Address Translation	involves re-writing the source and/or destination addresses of IP packets as they pass through a router or firewall

Acronym	Word/Phrase	Definition
NFR	Network Flight Recorder	Public domain software for providing information about network traffic and growth of the network, its usage patterns, bottlenecks, potential misconfigurations, etc.
NIST	National Institute of Standards and Technology	See: <a href="http://www.nist.gov">www.nist.gov</a>
NMS	Network Management Systems	A combination of hardware and software used to monitor and administer a network
NOC	Network Operations Center	GSA's Network Operations Center
OCIO	Office of the Chief Information Officer	The Office of the Chief Information Officer (OCIO) provides vision, leadership and expertise in Information Management (IM) and Information Technology (IT) critical to achieving GSA's business goals. See <a href="http://www.gsa.gov">www.gsa.gov</a>
OCONUS	Outside the Continental United States	Outside the Continental United States
OMB	Office of Management and Budget	See: <a href="http://www.OMB.gov">www.OMB.gov</a>
OSI	Open Systems Interconnection	A layered, abstract description for communications and computer network protocol design, developed as part of the Open Systems Interconnection initiative.
OSPF	Open Shortest Path First	A link-state, hierarchical <i>interior gateway protocol</i> (IGP) for network routing.
PBS	Public Buildings Service	GSA Public Buildings Service, see <a href="http://www.gsa.gov">www.gsa.gov</a>
PDA	Personal digital assistants	Handheld devices that were originally designed as personal organizers, but now include internet access and mobile phones.
PKI	Public Key Infrastructure	An arrangement that provides for trusted third party vetting of, and vouching for, user identities. It also allows binding of public keys to users
PMP	Program Management Plan	Defined in Appendix A Program Management Section 6.2 Program Management Plan
PPP	Point-to-Point Protocol	Commonly used to establish a direct connection between two nodes.
PPPoE	Point-to-Point Protocol over Ethernet,	A network protocol for encapsulating PPP frames in Ethernet frames. It is used mainly with ADSL services.

Acronym	Word/Phrase	Definition
PRI	Primary Rate Interfaces	A telecommunications standard for carrying multiple DS0 voice and data transmissions between two physical locations. All data and voice channels are ISDN and operate at 64 kbit/s.
PRS	Performance Requirements Summary	See attachment 18 and 26 of the PWS
PTP	Point To Point	Point-to-point data link is a communications medium with exactly two endpoints and usually no formatting. With respect to wireless data communications for Internet or Voice over IP it uses radio frequencies in the multi-gigahertz range.
PTT	Presidential Transition Team	A team established to facilitate the transition from one presidential administration to a newly elected one. This occurs once every four years.
PVC	Permanent Virtual Circuits	A dedicated circuit link in which data from a source user may be passed to a destination user over more than one real communications circuit during a single period of communication, but the switching is hidden from the users. A widely used virtual circuit protocol is the Transmission Control Protocol (TCP).
PWS	Performance Work Statement	A statement, which accurately reflects the government's requirements and declares the performance standards that can be used to evaluate that contractor performance is adequate and acceptable.
QA	Quality Assurance	It is the activity that ensures the quality of all processes and activities associated with the production of desired results.
QASP	Quality Assurance Plan	Defined in Attachment F of the PWS
QCP	Quality Control Plan	Defined in Cross-Cutting Section 19.12 Quality Control Plan
RAS	Remote Access Service	Defined in Appendix E Section 4.6
RFQ	Request for Quotation	An invitation for suppliers, through a bidding process, to bid on a specific product or service.
ROI	Return on Investment	A comparison of the money earned (or lost) on an investment to the amount of money invested.
sDSL	symmetrical DSL	This connection, doesn't allow the use of the phone at the same time, but enable DSL speeds for receiving and sending data.

Acronym	Word/Phrase	Definition
SNMP	Simple Network Management Protocol	Forms part of the internet protocol suite as defined by the Internet Engineering Task Force (IETF). More specifically, it is a Layer 7 or Application Layer protocol that is used by network management systems for monitoring network-attached devices for conditions that warrant administrative attention.
SOP	Standard Operating Procedures	A set of instructions having the force of a directive, covering those features of operations that lend themselves to a definite or standardized procedure without loss of effectiveness.
SPLAT	Signal Propagation, Loss, And Terrain	A RF Signal Propagation, Loss, And Terrain analysis tool
SQL	Structured Query Language	The most popular computer language used to create, modify, retrieve and manipulate data from relational database management systems.
SSO	Single Sign-On	Defined in Appendix B Section 5.3.4.8
STAR	System for Tracking and Administering Real Property	GSA PBS IT system for tracking real property.
STMP	Sub-Task Management Plan	Defined in Cross-Cutting Section 19.6 Sub-Task Management Plan
SVC	Switched Virtual Circuit	A virtual circuit that is dynamically established on demand and is torn down when transmission is complete
VLAN	Virtual Local Area Network	A method of creating independent logical networks within a physical network. Several VLANs can co-exist within such a network.
VoIP	Voice over Internet Protocol	The routing of voice conversations over the Internet or through any other IP-based network.
VPN	Virtual Private Network	A private communications network often used within a company, or by several companies or organizations, to communicate confidentially over a publicly accessible network
WABN	Wide Area Backbone Network	Defined in Appendix B Section 6.2
WAN	Wide Area Network	A computer network covering a broad geographical area. WANs are used to connect local area networks (LANs) together, so that users and computers in one location can communicate with users and computers in other locations.

Acronym	Word/Phrase	Definition
WBS	Work Breakdown Structure	An exhaustive, hierarchical (from general to specific) tree structure of deliverables and tasks that need to be performed to complete a project.
WIC	Wallace Incident Communicator	An incident management and crisis communication system. See <a href="http://www.wallacewireless.com">www.wallacewireless.com</a>
WINS	Windows Internet Naming Service	Microsoft's implementation of NetBIOS Name Server (NBNS) on Windows, a name server and service for NetBIOS computer names
xDSL	x Digital Subscriber Line (of any type)	The 'x' designates a DSL service of any type.

## Appendix G: Table of Attachments

Attachment 1:	Current Hardware Assets
Attachment 2:	Customer Locations and Counts
Attachment 3:	GSA Standard Client Hardware Configuration
Attachment 4:	GSA Technical Reference Model (TRM)
Attachment 5:	LCS Regional Network Topology - 04/10/2008
Attachment 6:	WAN diagram(s) and/or descriptions <ol style="list-style-type: none"><li>WAN US Map</li><li>WAN Typical Site Integration</li></ol>
Attachment 7:	LABN diagram(s) and/or descriptions <ol style="list-style-type: none"><li>Typical LABN Regional Site</li><li>GSA Regional Internet Access</li><li>GSA Regional Network Security</li></ol>
Attachment 8:	Office of Enterprise Infrastructure – 12/11/2007
Attachment 9:	GSA Standard Image
Attachment 10:	Active Directory Governance
Attachment 11:	AD Design document
Attachment 12:	GSA Ramp-Up Plan to OMB
Attachment 13:	Identity Management Provisioning Workflow
Attachment 14:	HSPD12 - Logical Access –04/9/2008
Attachment 15:	ID Management Architecture
Attachment 16:	ID Management Sample Workflow
Attachment 17:	Reserved
Attachment 18:	Performance Requirements Summary
Attachment 19a:	Security Guidance.zip <ul style="list-style-type: none"><li>• Windows 2003 Server Hardening Guide Package (CIO IT Security 04-25) – Rev. 2 – 06/21/2006</li><li>• CIO P 2100.1D GSA Information Technology (IT) Security Policy – 06/21/2007</li><li>• Access Control (CIO IT Security 01-07) – Rev. 2 - 01/30/2008</li><li>• Auditing &amp; Monitoring (CIO IT Security 01-08) – Rev. 2 - 01/29/2008</li><li>• CIO 2100.2 GSA Wireless Local Area Network (LAN) Security</li><li>• CIO 2100.3 Mandatory IT Security Training Requirement For Agency And Contractor Employees With Significant Security Responsibilities</li><li>• CIO 2104.1 GSA Information Technology (IT) General Rules of Behavior</li></ul>
Attachment 19b:	Security Guidance.zip <ul style="list-style-type: none"><li>• Microsoft IIS 5.0 Server Hardening Guide Package (CIO IT Security 02-18/19)</li><li>• GSA IIS Hardening Policy / Checklist (CIO IT Security 01-14)</li></ul>

- FISMA/POA&M Implementation (CIO-IT-Security-04-26 Revision 4) - 5/26/2005
  - GSA Windows NT Hardening Policy / Checklist (CIO IT Security 01-13)
- Attachment 19c: Security Guidance.zip:
- Windows 2000 Server Hardening Guide Package (CIO IT Security 02-16/17) - 7/06/2003
  - Termination Transfer Guide (CIO IT Security 03-23) – Rev. 2 – 01/29/08
  - GSA Contingency Plan Testing (CIO-IT-Security 06-29) 01/25/2006
  - Home User's Guide (CIO IT Security 04-24) - 9/29/2005
  - HSPD.doc
  - IT Security Procedural Guide: CISCO Router Hardening (CIO-IT Security-05-27) - March 8, 2005
  - IT Security Procedural Guide: IT Security Training and Awareness Program CIO-IT Security 05-29
  - IT Security Procedural Guide: Oracle Database Hardening (CIO-IT Security 05-28) - 3/29/2005
  - IT Security Procedural Guide: Windows 2000 Professional Hardening (CIO-IT Security 02-15) 11/16/2004, Revision 3
  - IT Security Procedural Guide: Windows XP Professional Hardening (CIO-IT Security 03-23)- 03/03/2006, Revision 6a
  - Managing Enterprise Risk (Security Categorization, Risk Assessment, & Certification and Accreditation) (CIO IT Security 06-30) – Rev. 4 – 10/16/2007
  - Password Generation and Protection (CIO IT Security 01-01) - 6/23/2005
  - Security Incident Handling Guide: (CIO IT Security 01-02) – Rev. 5 – 06/28/2007
  - Sun Solaris Server Hardening Guide Package (CIO IT Security 02-20)
- Attachment 19d: Other Guidance.zip:
- CIO 2160.2A GSA Electronic Messaging
  - CIO 2110.1 The "One GSA" Enterprise Architecture Policy
  - GSA Technical Reference Model (TRM) ("Bricks") – 09/07/2007
  - CIO 2161.1A Wireless Personal Digital Assistants (PDAs) – 09/26/2006
  - CIO 2160.3A Improving Desktop Management By Acquiring Standard Hardware and Software Configurations Using Electronic Business Processes – 07/18/2006
  - GSA Standard Image
  - GSA Privacy Act Program (CPO 1878.1 October 27,2003)
- Attachment 20: COOP Overview Information
- Attachment 21: Reserved
- Attachment 22: R1 Legacy Product Sets for Infrastructure Support
- Attachment 23: E-mail Infrastructure Diagrams V.0
- Attachment 24: BlackBerry Infrastructure – 04/01/2008

Attachment 25: WABN PVC  
Attachment 26: Incentivized Performance Requirements Summary  
Attachment 27: Voice Inventory