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

Contents

[1 Background 5](#_Toc17322421)

[1.1 <AGENCY> 5](#_Toc17322422)

[1.2 Project Background 6](#_Toc17322423)

[1.2.1 Environment 6](#_Toc17322424)

[1.2.2 Security Environment 7](#_Toc17322425)

[1.2.3 Cultural Environment 7](#_Toc17322426)

[1.2.4 Computing Environment and Technical Infrastructure Inventories 8](#_Toc17322427)

[2 Scope of Services 8](#_Toc17322428)

[3 Service Environment 8](#_Toc17322429)

[4 Work Statement 8](#_Toc17322430)

[4.1 Transition and Transformation Services 9](#_Toc17322431)

[4.1.1 Transition In 9](#_Toc17322432)

[4.1.2 Transition Out 10](#_Toc17322433)

[4.2 Contract, Program and Project Management Services 10](#_Toc17322434)

[4.2.1 Program Management Responsibilities 11](#_Toc17322435)

[4.2.2 Monitoring, Reporting and Review Services 13](#_Toc17322436)

[4.2.3 Security Management 14](#_Toc17322437)

[4.2.4 Planning and Analysis 16](#_Toc17322438)

[4.2.5 Integration and Testing 17](#_Toc17322439)

[4.2.6 Technical Change Management 19](#_Toc17322440)

[4.2.7 Capacity Management 20](#_Toc17322441)

[4.2.8 Asset Refresh and Provisioning 21](#_Toc17322442)

[4.2.9 Asset Acquisition and Network Services Provisioning 23](#_Toc17322443)

[4.2.10 Reports 23](#_Toc17322444)

[4.2.11 Project and Project Planning 25](#_Toc17322445)

[4.2.12 Project Oversight and Monitoring 25](#_Toc17322446)

[4.2.13 Weekly Project Status Meetings 25](#_Toc17322447)

[4.2.14 Financial Reviews 25](#_Toc17322448)

[4.2.15 Quarterly Executive Project Status Briefing 25](#_Toc17322449)

[4.2.16 Quality Assurance Surveillance Plan 26](#_Toc17322450)

[4.3 Personnel 26](#_Toc17322451)

[4.3.1 Key Personnel 26](#_Toc17322452)

[4.3.2 Staffing 26](#_Toc17322453)

[4.3.3 Warranty Services 27](#_Toc17322454)

[4.4 Policies, Procedures and Standards 27](#_Toc17322455)

[4.4.1 Standards and Common Practices 27](#_Toc17322456)

[4.4.2 After Hours Production Changes 28](#_Toc17322457)

[4.4.3 After Hours Support and Emergency Requirements 28](#_Toc17322458)

[4.4.4 Access to Government Facilities 28](#_Toc17322459)

[4.4.5 Records Maintenance and Reporting 28](#_Toc17322460)

[4.5 Facilities 29](#_Toc17322461)

[4.6 Operations and Maintenance 30](#_Toc17322462)

[4.6.1 Data Center 30](#_Toc17322463)

[4.6.2 Network 33](#_Toc17322464)

[4.6.3 Design/Engineering 34](#_Toc17322465)

[4.6.4 Implementation Services 35](#_Toc17322466)

[4.6.5 Operations and Administration 35](#_Toc17322467)

[4.6.6 Monitoring and Reporting 37](#_Toc17322468)

[4.6.7 Documentation 38](#_Toc17322469)

[4.7 Phone/Voice Support 38](#_Toc17322470)

[4.7.1 Desk Phone Service 39](#_Toc17322471)

[4.7.2 Telecommunications (Network, Conferencing and Voice) Services 39](#_Toc17322472)

[4.7.3 Voice Messaging 40](#_Toc17322473)

[4.7.4 Contact Center Service 41](#_Toc17322474)

[4.8 Enterprise Services 42](#_Toc17322475)

[4.8.1 Directory Service 42](#_Toc17322476)

[4.8.2 Identity Management 43](#_Toc17322477)

[4.8.3 Remote Access 43](#_Toc17322478)

[4.8.4 Desktop Management 44](#_Toc17322479)

[4.8.5 Core Software Build and Deployment Services 45](#_Toc17322480)

[4.8.6 Helpdesk Services 47](#_Toc17322481)

[4.8.7 Incident & Problem Management 48](#_Toc17322482)

[4.8.8 Root Cause Analysis 51](#_Toc17322483)

[4.9 Business Systems 51](#_Toc17322484)

[4.9.1 Database Management 52](#_Toc17322485)

[4.9.2 Service Recovery 54](#_Toc17322486)

[4.10 Projects 61](#_Toc17322487)

[4.11 Surge Labor 61](#_Toc17322488)

[4.12 Other Direct Costs / Travel 62](#_Toc17322489)

[4.13 Hardware / Tools 62](#_Toc17322490)

[4.14 Contract Access Fee 62](#_Toc17322491)

[5 Service Management 62](#_Toc17322492)

[5.1 Objectives 62](#_Toc17322493)

[5.2 Project Key Performance Parameters 63](#_Toc17322494)

[5.2.1 Customer Satisfaction Metric 63](#_Toc17322495)

[6 Referenced SOW Appendices and SOW Schedules 68](#_Toc17322496)

Information Technology Infrastructure Services

Statement of Work

# Background

## <AGENCY>

The (<AGENCY>) is an independent agency of the U.S. Government, established by XXX.

<AGENCY> funds research and education in science and engineering. It does this through grants, contracts, and cooperative agreements to more than XXX colleges, universities, and other research and/or education institutions in all parts of the United States. The Foundation accounts for about XX percent of federal support to academic institutions for basic research.

Each year, <AGENCY> receives approximately XXX new or renewal support proposals for research, graduate and postdoctoral fellowships, and math/science/engineering education projects; it makes approximately XXX new awards. These typically go to universities, colleges, academic consortia, nonprofit institutions, and small businesses.

<AGENCY> occupies XXX.

The XXX (the Board) is the governing board of <AGENCY>. The Board is composed of XX part- time members, appointed by the President and confirmed by the Senate. They are selected on the basis of their eminence in basic, medical, or social sciences, engineering, agriculture, education, research management or public affairs. The <AGENCY> Director serves on the Board, ex officio.

Other <AGENCY> senior officials include a Deputy Director who is appointed by the President with the advice and consent of the U.S. Senate, and eight Assistant Directors.

In addition to the Science Board, the Foundation is divided into over fifty organizational divisions that support the various staff and program offices and is structured as follows:

* + - * <AGENCY> Director
			* <AGENCY> Deputy Director
			* Seven staff Offices serving the Office of the Director
			* Seven Directorates
			* Two functional Offices oriented to financial or administrative support areas

The Foundation's mission is to fund research and education in science and engineering disciplines while supporting programs to strengthen the scientific and engineering research potential. Mission activities include receiving research proposals, conducting peer review through the use of panels or electronic messaging, and awarding funds to institutions and their principal investigators.

<AGENCY> does not conduct research or operate laboratories; however, through partnerships with other agencies, states, advisory committees, and academia, it funds research and education in science and engineering. It does this through grants, contracts, and cooperative agreements to more than 2,000 colleges, universities, and other research and/or education institutions in all parts of the United States.

The Foundation serves as a common ground for members of the scientific community by providing a collective point of information for current affairs and accounting for approximately 20 percent of federal support to academic institutions for basic research.

For more information about <AGENCY> please visit our website at [http://www.nsf.gov/.](http://www.nsf.gov/)

## Project Background

<AGENCY> is seeking to improve the availability, reliability, and scalability of its IT Infrastructure Services. These services include technology hosting, monitoring, remedial response, security, and network management. Many of these services and capabilities have become commodity businesses and <AGENCY> is seeking not only support of the current technical baseline, but also contemplates changes to its services concepts approach (see Attachment concerning projects). Last year, <AGENCY> successfully piloted the off-site technology-hosting concept with the deployment of Research.gov, and now plans to consolidate and upgrade data centers within a Government owned location. Hardware and software assets will remain the financial responsibility of <AGENCY> with operational responsibility sourced to the Contractor.

This acquisition will replace an existing contract providing on-site data center and infrastructure support services. In addition to performing operations and maintenance, it is expected that this acquisition will improve the support by providing high-availability service products in a networked environment. This acquisition will also provide several benefits to <AGENCY> including:

* + - * Improved operations management, strategic and tactical planning in providing these services.
			* Continuously improved performance, reliability, security of the delivered services through coordinated, proactive monitoring.
			* Adoption of proactive planning approaches to mitigating end-user problems.
			* Increased value of IT to <AGENCY> and its users through appropriate triage and escalation.

The Contractor shall plan and manage those activities necessary to transition services from the existing service provider. Optional tasks associated with this procurement include helping to plan and orchestrate migration to off-site hosting.

### Environment

<AGENCY> has a total workforce of about 1,700 at its XXX, headquarters, including approximately 1,200 career employees, 150 scientists from research institutions on temporary duty, 200 contract workers and the staff of the XXX office and the Office of the Inspector General. <AGENCY>’s population is varied and is heavily staffed by senior scientists. Nearly one-third of the senior scientists are on temporary (term) one to two (1-2) years duty at

<AGENCY>. Consequently, we have many employees who are sophisticated in computing, are pressured by their short tenure, and must learn our environment quickly in order to be productive. We also have a segment of staff, whether temporary (term) or permanent, who tend to explore and test new tools. Although the ultimate goal is to provide a standardized desktop computing environment, given this corporate culture, central-computing services must remain flexible and accommodating.

<AGENCY> supports a heterogeneous desktop environment; however, the standard

<AGENCY> desktop computer is a PC running Windows 7 that is configured via an <AGENCY> standard “image”, Microsoft Active Directory Group Polices, and an <AGENCY> “standard boot” network login procedure to meet the Government-wide Federal Desktop Core Configuration as well as <AGENCY>-specific requirements. <AGENCY> also supports a significant number of Macintosh desktop or laptop computers. <AGENCY>’s technological infrastructure is in a state of transition.

* + - * <AGENCY>’s standard set of application development tools is evolving from the Sun Application servers to BEA Application servers; from client-server applications to thin client (web) interfaces; and with respect to database management, <AGENCY> is moving from Sybase’s database management server to Oracle.
			* <AGENCY> intends to move current data center to a designated hosting facility.
			* <AGENCY> is working to ensure that we can proactively and effectively support changing desktop requirements while maintaining network security by restating and refining our desktop management approach.

### Security Environment

<AGENCY> maintains a defense-in-depth security environment that provides successive security controls as you progress through the security architecture. The <AGENCY> has a separate operational security group that is responsible for vulnerability management, monitoring and management of intrusion detection systems, along with incident response/ reporting.

<AGENCY> maintains a firewall, an intrusion detection capability, managed security services, active anti-virus/anti-spyware on the desktop. Laptops are encrypted for protection of data, web traffic is filtered, and a security event/log management to provide more incident detection capability is being deployed. <AGENCY> maintains an active vulnerability management program that includes scheduled and un-scheduled vulnerability scans each month, and a mature process for ensuring that identified vulnerabilities are analyzed and mitigated.

### Cultural Environment

Support teams must to be able to communicate with <AGENCY> staff and customers on a wide range of technical questions. Because <AGENCY> staff and customers represent a very wide range of computer skills, levels of responsibility, and job pressures, it is important to be sensitive to customer perception, to be tactful in tense situations, and to diffuse tensions and complaints. Support teams must listen attentively and patiently to a wide range of questions and requests; log them specifically and correctly; and respond with tact and consideration. Questions range from consultations that can be solved over the phone, to very complex problems or questions that may require escalation to the appropriate specialist(s).

Customer follow-up and proper closure is considered a necessary condition in the delivery of quality and timely customer service. Customer satisfaction is paramount. <AGENCY> cannot stress enough the importance of our customer service support programs to ensure a positive customer experience.

### Computing Environment and Technical Infrastructure Inventories

For a complete inventory of all software and hardware, reference the Current Hardware Inventory in Appendix XXX and the Current Software Inventory in Appendix XXX.

# Scope of Services

The Contractor shall provide support to the Government’s contracting representative(s) and project team by supporting areas of operational significance called out within this document. The first objective of Contractor support is to provide resources for the operations and maintenance of the servers, software, network components, image management, asset refresh (non-financial), operational security and FISMA compliance, and second-level support to the helpdesk. These services are described in Part I of the document and comprise the ‘core’ set of services and are the primary purpose for the acquisition. Secondary support services are described in Part II and are intended to capture administrative support functions (e.g., ITIL-like services, support during application testing, Disaster Recovery, etc.). Part III of this document identifies services required as project related support. From time to time <AGENCY> may request Project related activities necessary to modifying processes, implementing new technologies (e.g., major changes, such as IPV6) or projects requiring significant application of resources to meet Information Technology changes. These services are organized into eight areas of support:

* + - * Transition and Transformation Services
			* Contract, Program and Project Management Services
			* Operations and Maintenance Services
			* Projects
			* Surge Labor
			* Other Direct Costs / Travel
			* Hardware / Tools
			* Contract Access Fee

At all times, the Government will retain primary technical responsibility for the technical direction of the work described herein.

[Describe number of organizations, locations, and users]

# Service Environment

[Describe the IT Infrastructure Service environment (Hardware, Software, Tools, etc.)].

# Work Statement

## Transition and Transformation Services

### Transition In

The Contractor shall be responsible for transitioning current operational responsibilities and open projects to its control. Transition activities include planning, discovery, and programmatic functions (e.g., Contract Management, Human Resource Management, Quality Assurance, etc.) necessary to transfer all logistical and technical support to the new Contractor’s operations.

Transition shall include all activities necessary to establish Back Office Support (e.g., finance and accounting) or to other Contractor resources (e.g., Personnel, Sub-Contractors, Vendors).

At a minimum, the Contractor shall be responsible for and produce a plan that addresses steps / phases of implementation; time management; controls for managing cost, schedule, risk; and identifying any requirements that might be placed upon Government or other parties.

The transition preparation and phase-in period shall be 90 calendar days. During this period, the Contractor shall plan and manage those activities necessary to transition service from the existing service provider. Immediately after the notice to commence work, the Contractor shall perform due diligence through inventory of all <AGENCY> assets, system configuration information, current operations, and documentation. The Contractor shall document and provide findings to the Government in a Transition Plan. The plan shall include what has been accomplished related to the transition and what remains outstanding, including any issues that need to be addressed. The Transition Plan shall transfer service responsibility to the Contractor at the end of the maximum ninety-day (90-day) transition timeframe, upon which the Contractor shall assume responsibility for operational, technical, and financial performance.

Objectives for transition include:

* + - * No break in current service levels,
			* No delay in support for new and ongoing projects, and
			* Existing <AGENCY> projects shall continue as is, unless the Government directs changes.

During the phase-in period, the Contractor shall organize, plan, and recruit personnel for remaining outstanding positions as well as mobilize resources, develop procedures, and accomplish all actions necessary to commence full performance of the services at the end of the transition period.

During the phase-in period, the Contractor shall:

1. Establish project management procedures and review Standard Operating Procedures (SOPs). Note: most IT Infrastructure process have not been captured in SOPs. In the instances where SOPs have not been documented, the Contractor will be expected to create SOPs during the transition period by capturing existing knowledge from the incumbent vendor.
2. Recruit, hire, and on-board necessary personnel.
3. Attend post-award meetings as required.
4. Create SOPs for each functional area covered under this SOW. Content may include: Quality Control (QC), work assignments, approval authorities, workflow, functional relationships between the Government and the Contractor, functional relationships between the Contractors’ organizational elements (including subcontractors), and any other information needed for efficient and uniform performance.

***Deliverables***

1. Draft Transition Plan (as proposed by the Contractor in the response to the SOW)
2. Final Transition Plan (as accepted by the Government, after contract award)
3. Resource Plan
4. Resource report
5. Daily status report
6. SOPs for each SOW functional area
7. Updates to existing SOPs
8. Draft service performance measures
9. Final service performance measures

The Contractors shall provide a statement of assumption of Full Operational Capability (FOC) upon completion of the Transition In period.

### Transition Out

Toward the end of the Contract term, the Contractor may be required to support a successor Contractor, see FAR 52.237-3. In addition, during contract performance the Government’s needs or requirements could potentially alter the support efforts required by this contract. The Contractor shall cooperate to affect an effective, orderly, and efficient Transition-In / Transition- Out to any such successor Contractor during a Transition-In / Transition-Out period to be specified by the Contracting Officer. The Contractor shall be required to phase out the existing contract turning over total contract control to the new Contractor in a well-organized, systematic, and planned manner. The incumbent Contractor shall meet as necessary with the new Contractor. All Contractor personnel shall support the efforts established by the Transition-In / Transition-Out Team. Both Contractors shall develop a joint Transition-In / Transition-Out Plan of critical areas to be satisfied, that will be initialed and dated by both parties.

The Contractors shall provide a statement of transition of Full Operational Capability (FOC) upon completion of the Transition Out period.

## Contract, Program and Project Management Services

Program and project management services includes contract administration and compliance, audit, back-office related activities (e.g., invoicing), account management, program management, and other recurring routine functional tasks to plan, control and ensure technical objectives are delivered on schedule and within defined budgets. These services include a number of common Information Technology life cycle support and management practices that the Contractor shall provide by coordinating and communicating Solution Engineering, Maintenance, and Operational activities with other Contractors and ITIS personnel performing work across all service areas. PM ITIS intends to maintain a high-performing organization with integrated project teams and cross-functional services that will leverage such practices – which will be tantamount to achieving the objectives set-forth in the Section below.

### Program Management Responsibilities

The <AGENCY> Program Management Office (PMO) requires the use of systematic program and project management methodology with all IT support activities. The methodologies shall use frameworks based on the Project Management Institute (PMI) frameworks for project management. The Contractor shall maintain data and information that relates technical components of infrastructure with business requirements. Business management and reporting shall focus project activities and their impact on budgeted work, planning and control, overall performance, and conformance to contractual requirements. The technical component shall focus on areas such as data gathering, requirements definition; technical design; development; testing, installation, interoperability, operational support, and management of software as Government asset.

The Contractor shall provide the day-to-day management of the project and deliver the means, methods, and resources to meet the Contract end point requirements and the intermediate requirements that the Contracting Officer’s Technical Representative (COTR) and/or Performance Monitor(s) determined are value-added and necessary to achieve project success.

The following table identifies program management roles and responsibilities associated with the Administrative Support Services.

Table . Project Management Roles and Responsibilities

| **Project Management Roles and Responsibilities** | **Provider** | **<AGENCY>** |
| --- | --- | --- |
| 1. Information Resource Management Strategic Plan, Circular A-130, and OMB 300 requirements
 | No | Yes |
| 1. Provide services that support <AGENCY> business needs, technical requirements end-user requirements in planning and reporting under the <AGENCY> strategic plan for Information Resource Management.
 | Yes | No |
| 1. Comply with <AGENCY> policies and standards and regulations applicable to <AGENCY> for information, information systems, personnel and resource management, physical and logical security.
 | Yes | No |
| 1. Develop, maintain, and communicate the Contractor’s practices, support organizations, and support personnel contacts related to the Contractor’s operations used in the delivery of solution engineering services.
 | Yes | No |
| 1. Provision quarterly account management reviews between <AGENCY> Executives and Contractor Executive personnel.
 | Yes | No |
| 1. Identify activities and dependencies where the Contractor has reliance on <AGENCY> and / or 3rd party resources, tools, and processes.
 | Yes | No |
| 1. Communicate opportunities and / or risks associated with identified activities and dependencies for which the Contractor has reliance on other parties.
 | Yes | No |
| 1. Provide administrative access of Contractor Dashboard and/or management information to <AGENCY> personnel and IV&V personnel.
 | Yes | No |
| 1. Segregation of costs and activities by job codes to permit management and reporting of labor hour expenditures and tracking of allocations, or other resources and related costs.
 | Yes | No |
| 1. Ensure sufficient cost visibility for both the Government and the Contractor to ensure quality across all activities (e.g., Transition, Implementation, operational concepts, and any disengagement support).
 | Yes | No |
| 1. Responsibility for accumulating data, tracking, and reporting on performance, deliverables, and <AGENCY> costs.
 | Yes | No |
| 1. Provide appropriate levels of skilled and knowledgeable resources necessary to meet service objectives and requirements of the SOW – including unplanned surges in workload (e.g., emergencies, projects, backlog).
 | Yes | No |
| 1. Control all performance, deliverables, schedules, and cost, for projects and immediately advise the COTR, Contract Officer (CO), and designated Performance Monitors, as appropriate, of any problem(s) that arise or may imperil or impede the Task Order or task performance.
 | Yes | No |
| 1. Provide impact assessments (e.g., financial impact, risk, resource levels) for all change requests or regulatory.
 | Yes | No |
| 1. Approval of changes or actions (subject to COTR, CO)
 | No | Yes |
| 1. Attend meetings and / or conferences as required by <AGENCY> or is necessary to conform to regulatory requirements.
 | Yes | No |
| 1. Availability during normal hours of operation to plan, direct, and control the overall management functions.
 | Yes | No |
| 1. Within 30-minute notice, during normal work hours, meet with the COTR, in person or as otherwise agreed upon by the COTR, to discuss status or problems. After normal working hours, the COTR or designated alternate shall be available within 60 minutes after notification to coordinate any necessary actions.
 | Yes | No |
| 1. Provide daily status, weekly summaries, and detailed project reviews showing, at a minimum: Schedule attainment, cost projections, planned activities, accomplishments, and risks.
 | Yes | No |

### Monitoring, Reporting and Review Services

Monitoring and reporting services are the activities associated with the ongoing health checks, status reporting, and problem management (ongoing surveillance, tracking, escalation, resolution, and tracking of problems) of application support activities. Problem Management activities described within this document require the Contractor to provide Level 2 technical support in coordination with the Help Desk. Unless otherwise stated in this SOW, all forms of reports to be provided by the Contractor in accomplishment of the work described herein shall be pre-approved during the Transition period by <AGENCY>.

The following table identifies the underlying roles and responsibilities associated with Monitoring, Reporting and Review activities.

Table - Monitoring, Reporting and Review Services Roles and Responsibilities

| **Monitoring, Reporting and Review Services Roles and Responsibilities** | **Provider** | **<AGENCY>** |
| --- | --- | --- |
| 1. Provide, maintain, and update project plans, identifying critical path dependencies, major critical milestones, project deliverables, and tracking (e.g., project earned value) for Projects and for ongoing Service Delivery.
 | Yes | No |
| 1. COTR determination as to whether EVM shall apply to projects.
 | No | Yes |
| 1. Provide weekly status reviews and progress reports.
 | Yes | No |
| 1. Provide monthly service-level performance reports against each SLR, including trends for each and summary view.
 | Yes | No |
| 1. Provide monthly milestone achievement review and performance reports.
 | Yes | No |
| 1. Provide mutually agreed to reports to enable invoice reconciliation.
 | Yes | No |
| 1. Provide mutually agreed to reports that capture Service Requests demands and measure of ability to satisfy demand.
 | Yes | No |
| 1. Define SLR, problem Severity Levels, and reporting cycles.
 | No | Yes |
| 1. Measure and analyze performance relative to requirements.
 | Yes | No |
| 1. Develop improvement plans for services that do not meet SLR.
 | Yes | No |
| 1. Review and approve improvement SLR plans.
 | No | Yes |
| 1. Implement improvement SLR plans.
 | Yes | No |
| 1. Participate and support Security Reviews, IV&V, and / or Quality Assurance (QA) compliance assessments.
 | Yes | No |
| 1. Support reviews for Authority to Operate and / or Accreditation Reviews per NIST 800-53A.
 | Yes | No |
| 1. Report on participation in Technical Interchange Meetings (TIM) for exchanges on new technology insertion, functional requests, and change control meetings (e.g., impact on interoperability, risks, and recommendations).
 | Yes | No |

### Security Management

Security Management services includes physical and logical security of all application components and data, access protection and other security services in compliance with <AGENCY> Security requirements and all applicable regulatory requirements.

The following table identifies Security Management roles and responsibilities associated with Service Delivery.

Table – Security Management Roles and Responsibilities

| **Security Management Roles and Responsibilities** | **Provider** | **<AGENCY>** |
| --- | --- | --- |
| 1. Define security requirements, standards, procedures, and policies including regulatory requirements.
 | No | Yes |
| 1. Where required by <AGENCY> participate in industry security forums and users’ groups to remain up to date with current security trends, threats, common exploits and security policies and procedures.
 | Yes | No |
| 1. Assist in developing security standards, policies, and procedures including industry best practices.
 | Yes | No |
| 1. Work with Security Team and conduct risk assessment to identify control or security gaps.
 | Yes | No |
| 1. Document IT security practices and plans based upon standards and practices, <AGENCY> policies, and federal requirements.
 | Yes | No |
| 1. Review and approve security plans.
 | No | Yes |
| 1. Implement physical and logical security plans consistent with <AGENCY> security policies and industry standards / practices (e.g., FISMA, NIST, ISO, other authoritative frameworks, and organizations).
 | Yes | No |
| 1. Establish access profiles and policies for adding, changing, enabling/disabling, and deleting log-on access of <AGENCY> employees, agents, and subcontractors.
 | No | Yes |
| 1. Implement log-on/security-level access changes as detailed in profiles and policies.
 | Yes | No |
| 1. Report security violations to <AGENCY> within parameters of <AGENCY> policies.
 | Yes | No |
| 1. Final disposition on security violations
 | No | Yes |
| 1. Work with <AGENCY> Senior Information Systems Security Officer (SISSO) and Security Teams to resolve security violations that originate outside of the hosted network(s) (e.g., denial of service attacks, spoofing, Web exploits).
 | Yes | No |
| 1. Review all security patches relevant to the IT environment and classify the need and speed in which the security patches should be installed as defined by security policies.
 | Yes | No |
| 1. Install security patches within 48 hours, or as otherwise directed by the <AGENCY>.
 | Yes | No |
| 1. Perform testing in conjunction with security patch deployment.
 | Yes | No |
| 1. Participate in periodic security 3rd party audits.
 | Yes | No |
| 1. Maintain all documentation required for security audits and internal control and control testing.
 | Yes | No |
| 1. Place and support systems with particularly sensitive data in controlled access areas. Only Users with current, authorized access permission will be allowed to enter these areas.
 | Yes | No |
| 1. Cooperate with 3rd party security audits.
 | Yes | No |

### Planning and Analysis

Planning and analysis services are the activities associated with the research and application of new technologies, trends, and changes in market conditions; and include investigation of opportunities to improve the efficiency, effectiveness and quality of <AGENCY>’s Infrastructure.

The following table identifies the roles and responsibilities associated with Planning and Analysis services.

Table – Planning and Analysis Roles and Responsibilities

| **Planning and Analysis Roles and Responsibilities** | **Provider** | **<AGENCY>** |
| --- | --- | --- |
| 1. Assess processes and methodologies.
 | Yes | No |
| 1. Audit and Validation of process and methods.
 | No | Yes |
| 1. Conduct semiannual technical reviews. One review shall be completed no later than 30 days prior to the anniversary date of the contract and the second at the midpoint of each contract year.
 | Yes | No |
| 1. Maintain Technical Baseline.
 | Yes | No |
| 1. Monitor technical trends through independent research; document and report on products and services with potential use for <AGENCY>.
 | Yes | No |
| 1. Perform business liaison function to operational units.
 | Yes | No |
| 1. Perform business planning for capacity and performance in advance of annual <AGENCY> financial planning.
 | Yes | No |
| 1. Provide quarterly updates on capacity and performance against annual plans.
 | Yes | No |
| 1. Approve Plans and changes to capacity.
 | No | Yes |
| 1. Recommend overall systems development life cycle process improvements, including those for which <AGENCY> retains responsibility.
 | Yes | No |
| 1. Perform an annual portfolio analysis to identify and recommend applications rationalization, consolidation, sun-setting, etc. [conduct within 30 days after each contract renewal period (i.e., option period) or COTR’s request].
 | Yes | No |
| 1. Facilitate annual technical interchanges and business planning sessions to establish standards, architecture, and project initiatives.
 | Yes | No |
| 1. Participate in annual technical interchanges and business planning sessions to establish standards, architecture, and project initiatives.
 | Yes | No |
| 1. Identify possible product and software tool enhancement opportunities for improved performance, stability, and potential cost savings.
 | Yes | No |

### Integration and Testing

Integration and testing services are the activities associated with the confirmation that 1) individual components work together properly with its’ associated system or within the collective body of <AGENCY> systems and architecture, 2) as a whole the Contractor shall ensure that systems and components (hardware and software) shall perform to their specified functions and contractual service requirements, 3) meet all performance requirements specified in tests plans, are interoperable with platforms and products incorporated into the design, and 4) meet any security /auditability requirements. This includes application interfaces to other applications and/ or other platforms already in production at or being developed by <AGENCY>, or connectivity with outside parties as stated in the requirements documents.

The following table identifies the roles and responsibilities associated with Integration and Testing services.

Table – Integration and Testing Roles and Responsibilities

| **Integration and Testing Roles and Responsibilities** | **Provider** | **<AGENCY>** |
| --- | --- | --- |
| 1. Approve all plans for integration and acceptance of systems and component changes, security reviews, and changes and test plans for new and upgraded equipment, software, or services.
 | No | Yes |
| 1. Create test plans, test data, and perform all appropriate testing (component testing, system tests, and end-to-end testing).
 | Yes | No |
| 1. Review and approve testing processes, schedules, and recommendations.
 | No | Yes |
| 1. Coordinate multi-source tests (e.g., applications with infrastructure and establish and define acceptance criteria, test objectives, parameters, and risks).
 | Yes | No |
| 1. Facilitate troubleshooting support to test teams and users.
 | Yes | No |
| 1. Conduct user, non-user acceptance testing and other types of testing.
 | Yes | No |
| 1. Assist security team in performing tests for certification and accreditation.
 | Yes | No |
| 1. Document and update Quality Assurance Plan (QAP) and quality controls with lessons learned.
 | Yes | No |
| 1. Validate all new and upgraded software or services for compliance with <AGENCY> application Security policies and instructions.
 | Yes | No |
| 1. Create real or virtual test environments for Application software tests as required by Application Developers.
 | Yes | No |
| 1. Support Application Development teams with IT Infrastructure requirements and impact to current systems and capacity.
 | Yes | No |
| 1. Review testing results for compliance with policies, procedures, plans, and test criteria and metrics (e.g., defect rates, progress against schedule, etc.).
 | No | Yes |
| 1. Notify Contractor in the event <AGENCY> notices a discrepancy between <AGENCY>’s requirements and the requirements document or Contractor deliverables.
 | No | Yes |
| 1. Correct defects found as a result of testing efforts and retest.
 | Yes | No |
| 1. Conduct selective random independent testing.
 | No | Yes |
| 1. Documentation (e.g., Implementation and preparation guidance and coordination of implementation risks with service delivery groups).
 | Yes | No |
| 1. Stage systems before implementation (hardware refresh, software updates, or new systems – as determined by project).
 | Yes | No |
| 1. Support and ensure preparation of <AGENCY> production environments for implementation.
 | Yes | No |

### Technical Change Management

Technical Change Management activities include services required to appropriately manage and document (e.g., impact analysis, version control, library management, turnover management, build management, parallel development) changes to configurations and any of the constituent peripherals. Technical Change Management also includes services required to appropriately manage and document changes to the underlying components of systems.

Any changes to the baseline project plan or committed maintenance or enhancement dates must be managed by the Technical Change Management process and approved by

<AGENCY>. This shall include systems and methods for formal and documented Technical Change Management procedures, document management, tracking of assets and approval levels necessary to authorize changes (e.g., a change to the scheduled end date for a particular work product). The Contractor shall utilize <AGENCY> change request (CR) process, which includes a standard form describing the type of change/issue, the rationale behind it, and related schedule and cost changes.

The following table identifies the roles and responsibilities associated with Technical Change Management services.

Table – Technical Change Management Roles and Responsibilities

| **Technical Change Management Roles and Responsibilities** | **Provider** | **<AGENCY>** |
| --- | --- | --- |
| 1. Prepare all <AGENCY> change requests using [insert tool].
 | Yes | No |
| 1. Approve system changes.
 | Yes | No |
| 1. Update asset management records, monitor usage, and provide asset management support in monitoring licenses for expiration, idled status, or other issues. Notify the COTR as soon as such issues are discovered.
 | Yes | No |

### Capacity Management

Capacity Management is responsible for ensuring that the capacity of the Contractor team’s ability to perform matches the evolving demands of <AGENCY> business in the most cost- effective and timely manner. The process encompasses the following:

* + - * Monitoring of performance and throughput of IT services and supporting IT components.
			* Understanding current demands and forecasting for future requirements.
			* Developing capacity plans which will meet demand and Service Level Requirements (SLR).
			* Conducting risk assessment of capacity recommendations.
			* Identifying financial impacts of capacity plans.
			* Undertaking tuning activities.
			* Development of long- and short-term staffing plans.
			* Adherence to <AGENCY> priorities.

The following table identifies Capacity Management roles and responsibilities associated with Service Delivery.

Table - Capacity Management Roles and Responsibilities

| **Capacity Management Roles and Responsibilities** | **Provider** | **<AGENCY>** |
| --- | --- | --- |
| 1. Establish comprehensive capacity management planning process.
 | No | Yes |
| 1. Review and approve capacity management planning process.
 | No | Yes |
| 1. Define, develop, and implement tools that allow for the effective capacity monitoring/trending of applications and IT components.
 | Yes | No |
| 1. Identify future business requirements that will alter capacity requirements.
 | No | Yes |
| 1. During the Transition period the Contractor shall prepare and provide to <AGENCY> a ninety (90) day rolling forecast of resource demand and capacity.
 | Yes | No |
| 1. Update capacity plans as required.
 | Yes | No |
| 1. Assess capacity impacts when adding, removing, or modifying applications.
 | Yes | No |
| 1. Continually monitor IT resource usage to enable proactive identification of capacity and performance issues.
 | Yes | No |
| 1. Capture trending information and forecast future <AGENCY> capacity requirements based on <AGENCY> defined thresholds.
 | Yes | No |
| 1. Recommend and forecast changes to capacity to improve service performance.
 | Yes | No |
| 1. Assess impact/risk and cost of capacity changes as it relates to in scope activities.
 | Yes | No |
| 1. Approve capacity related recommendations.
 | No | Yes |
| 1. Maintain capacity levels to optimize use of existing IT resources and minimize <AGENCY> costs to deliver services at agreed to SLR.
 | Yes | No |
| 1. Ensure adequate capacity exists within the IT environment to meet SLR requirements taking into account daily, weekly, and seasonal variations in capacity demands.
 | Yes | No |

### Asset Refresh and Provisioning

<AGENCY>, at all times, will retain financial responsibility for all assets (hardware and software), and for architectural decisions governing the selection, distribution, and use of all systems, peripherals, and personal use equipment. Additionally, <AGENCY> shall retain all decision authority on asset management, changes, and refresh schedules. If the Government PMO requires assistance from the Contractor in such decisions then the Contractor shall participate and support the Government by providing research, impact assessments, deployment planning and documentation, and post-deployment assessments and documentation.

Provisioning – defined as the successful inclusion of new users or new systems into the enterprise <AGENCY> system as services are completed. It includes Integration and installation activities with Production Teams to ensure successful provisioning and starts with planning and coordination of moves and/or installations and continues after deployment into operational sustainment. Provisioning includes *Interim User Provisioning Processes*, beginning- to-end asset management (e.g., system builds, imaging, checkout, testing, maintenance, and disposal) of Government furnished equipment.

Table – Asset Refresh Provisioning Roles and Responsiblities

| **Asset Refresh and Provisioning Responsibilities** | **Provider** | **<AGENCY>** |
| --- | --- | --- |
| 1. Procurement of hardware and software Assets (financial and licenses)
 | No | Yes |
| 1. Creation of user or system authorizations, image and other software loading aligned with organization tiers and mappings (e.g., network, authentications, passwords, etc.) and documentation/user records to appropriate systems within <AGENCY>
 | Yes | No |
| 1. Manage suspension of user access and chain-of-custody when required by <AGENCY>.
 | Yes | No |
| 1. Provisioning decisions and approval of Authorizations
 | No | Yes |
| 1. Provide provisioning metrics, as requested by the COTR.
 | Yes | No |
| 1. Coordinate warranty items (e.g., parts).
 | Yes | No |
| 1. Manage user lists for errors and perform account creation and deletion.
 | Yes | No |
| 1. Manage asset tags, user profiles, and records within <AGENCY> systems.
 | Yes | No |
| 1. De-install systems and prepare hardware for disposal.
 | Yes | No |
| 1. Perform necessary actions to reclaim software licenses.
 | Yes | No |
| 1. Disposal decision
 | No | Yes |

### Asset Acquisition and Network Services Provisioning

Provider will perform Asset Acquisition and Network Services Provisioning associated with acquiring network equipment and circuits.

The following table identifies the underlying roles and responsibilities associated with Asset Acquisition and Network Service Provisioning activities.

Table – Asset Acquisition and Network Service Provisioning Roles and Responsibilities

| **Network Provisioning Roles and Responsibilities** | **Provider** | **<AGENCY>** |
| --- | --- | --- |
| 1. Order and expedite WAN circuits, equipment, and services.
 | No | Yes |
| 1. Manage logistics for WAN circuits, equipment, and services.
 | Yes | No |
| 1. Configure WAN/LAN (hardware, software) prior to installation.
 | Yes | No |
| 1. Provide test plans for new equipment and circuits and perform/support tests as required by <AGENCY>.
 | Yes | No |
| 1. Document router configuration files and IP addressing schemas.
 | Yes | No |
| 1. Define network provisioning requirements and use policies.
 | No | Yes |
| 1. Manage network provisioning requirements and use to policies.
 | Yes | No |
| 1. Provide capacity planning assistance to develop network resource requirements projections.
 | Yes | No |
| 1. Manage the performance of public carriers (and other 3rd parties) to meet defined schedules, project plans, Service Level Requirements, etc.
 | Yes | No |
| 1. Ensure that all new circuits, devices, and software provisioned are included in configuration management documentation.
 | Yes | No |

### Reports

The Contractor shall provide written reports to <AGENCY> regarding Contractor’s compliance with the service management conditions specified Section [XXX](#_bookmark55).

In addition, the reports shown in the table below are required.

Table - Reports

| **Description** | **Timing** |
| --- | --- |
| 1. Weekly Status Review and Progress Reports (see [Table 2](#_bookmark16))
 | Weekly |
| 1. Monthly Service Level Performance Reports (see [Table 2](#_bookmark16))
 | Monthly |
| 1. Monthly Milestone Achievement and Performance Reports (see [Table 2](#_bookmark16))
 | Monthly |
| 1. Monthly Invoice Reconciliation Reports (see [Table 2](#_bookmark16))
 | Monthly |
| 1. Monthly Status Report (see [Table 2](#_bookmark16))
 | Monthly |
| 1. Monthly Service Request Time Management Report (see [Table 2](#_bookmark16))
 | Monthly |
| 1. 90 Rolling Forecast Resource Demand and Capacity Report (see [Table 7](#_bookmark22))
 | Monthly |
| 1. Monthly financial and project progress reports for use in the Government IT Dashboard reports (details provided on a case by case application basis)
 | Monthly |
| 1. Schedule including planned and actual performance Major tasks completed and deliverables provided during the period
 | Monthly |
| 1. Major tasks and deliverables planned for the next reporting period
 | Monthly |
| 1. Summary and supporting funds status showing costs of resources and planned burn rate, travel, ODCs
 | Monthly |
| 1. Potential risks, risk assessments, and proposed mitigations, including status on established mitigations and schedules for proposed ones
 | Monthly |
| 1. Potential and actual problems, and proposed ‘work-around’ and solutions, including time frames
 | Monthly |
| 1. Problems and issues requiring <AGENCY> management attention
 | Monthly |
| 1. Quality Assurance Surveillance Plan reporting results
 | Monthly |
| 1. Schedule Variance and Performance Reporting
 | Monthly |
| 1. Quarterly Property Management Report (see Sections [0,](#_bookmark20) [0,](#_bookmark27) [0](#_bookmark23)
2. and [Table 6](#_bookmark21))
 | Quarterly |
| 1. Quarterly Software License Inventory Report (see Sections XXX and [Table XXX](#_bookmark21))
 | Quarterly |
| 1. Quarterly Capacity and Performance Report (see [Table XXX](#_bookmark18))
 | Quarterly |
| 1. Semi-Annual Technical Review (see [Table XXX](#_bookmark18))
 | Semi-Annual |
| 1. Annual Portfolio Analysis (see [Table XXX](#_bookmark18))
 | Annual |

### Project and Project Planning

From time-to-time <AGENCY> may require project planning and artifacts for special projects. In such situations the Contractor shall develop a product-oriented project plan that provides the Government in-sight into the proposed efforts. The project plan must include, at a minimum:

* + - * Work Breakdown Structure (WBS), which defines the entire project scope and establishes how the work will be accomplished by breaking down the project into its component elements. The WBS shall break the work down into work packages - manageable units that can be planned, budgeted, scheduled, and controlled. The WBS should have a WBS dictionary, which contains information about each work package such as schedule dates and fixed hourly rates.
			* For project related activities the Contractor shall develop and provide a Milestone chart which focuses on the initiation and conclusion of major program milestones as key events.
			* The Contractor shall provide a milestone table to include each of the project increments, releases and Pre-Production and Production performance.

### Project Oversight and Monitoring

<AGENCY> expects to monitor project progress through status meetings and reports, financial re-views, and executive briefings. The Contractor’s responsibilities related to project progress are described below.

### Weekly Project Status Meetings

The Contractor project manager shall meet weekly with the <AGENCY> project manager and with other appropriate <AGENCY> personnel to discuss project status, resolve issues, and address administrative matters and the like.

### Financial Reviews

The Contractor shall provide the <AGENCY> project manager with a detailed walk-through of monthly invoices as well as additional supporting information in the form of a financial status report. The financial status report shall provide (at a minimum) work hours and cost information (cumulative and for the invoice period) by CLIN, labor category, and Contractor name. Also, both planned and actual costs shall be presented by labor category within each CLIN.

### Quarterly Executive Project Status Briefing

The Contractor shall provide a quarterly project status briefing to <AGENCY> senior management. The briefing will be scheduled by the <AGENCY> COTR.

### Quality Assurance Surveillance Plan

The Contractor shall develop and maintain a Quality Assurance Surveillance Plan (QASP) that is organized and oriented to each service area (e.g., Data Center, Network, etc.) and for which shall address approaches to monitoring and managing performance. The QASP shall contain key indicators that will be used to manage performance and for identifying risk to <AGENCY>’s Enterprise Architecture methodology. The QASP shall be directly tied to each of the Service Areas and provide the Government insight into the proposed effort and illustrate Total Program performance standards, measurement techniques, and incentives/disincentives. The QASP will be evaluated initially to assure completeness of the anticipated deliverables list and the forecast dates of their delivery enabling appropriate Government validation.

This QASP shall outline the Contractor’s approach for monitoring and measuring activities – only for the Contractor but also where the Contractor is dependent on other parties, or where it uses contracted labor. The Contractor’s QASP shall detail performance requirements, establish a performance objective and the acceptable deviation from the objective in terms of acceptable quality levels. Also provide key outcomes for the program, the collection and assessment of the data shall be done by the Contractor.

## Personnel

### Key Personnel

At a minimum, the <AGENCY> expects the following roles to be associated with key personnel:

* + - * Project Manager
			* Functional Manager
			* Technical Manager

Team Leaders to include, as a minimum: deployment, help desk, testing, architecture, security, and training.

### Staffing

The Government desires programmatic leadership, technical expertise, and capabilities for proactively identifying, promoting, implementing, and communicating the advancement of solution engineering and maintenance. As such, the Contractor is encouraged to:

* Provide a team of experienced resources that can fulfill a variety of activities ranging from subject matter disciplines and research to expertise and skills in planning and implementation.
* Provide flexibility in resources assigned. That is, where appropriate, maintain continuity through a permanent mix of senior-, mid-, and junior-level staff experienced in supporting requirements in an environment similar to the size and complexity of <AGENCY>. However, as technologies change, PM <AGENCY> expects that the Contractor will maintain alignment by adjusting permanent resources and/or providing ad hoc expertise for projects and other short-term assignments.
* Establish continuous support and continuity through cross-training to ensure there are no impacts due to planned or unplanned staff changes.
* Be proactive in establishing and maintaining operational guides that document the

<AGENCY> organization, responsibilities, and processes that can be used to train resources, transfer knowledge, and create the basis for knowledge management.

* Replace, modify, and/or add staffing resources as needed in a timely, profession and consistent manner.

### Warranty Services

Warranty Services are the activities associated with correcting defects attributable to Contractor errors or negligence that are discovered within the Warranty Period of the deliverables, project work, or routine operational activities. The Warranty Period shall be for a minimum of 90-days after delivery and defined to begin at the time that project work is completed, deliverables are formally accepted by the authorized Government representative, or completion of routine work activities.

Warranty Services include the applicable life cycle support activities, as well as any activities necessary to repair errors/defects to enable systems to perform in accordance with OEM documentation, project specifications, or documented operational functionality.

The Contractor shall rework errors and defects at no charge to <AGENCY> provided that:

* + - * The problem encountered occurs within the Warranty Period and
			* The problem results in or reveals a Level 1 Incident or Nonconformity, or
			* The Contractor cannot demonstrate root cause attributable to other inputs

A level 1 Incident or Nonconformity is defined as, two (2) or more Customers impacted or potentially impacted by the same issue and/or Critical business impacted. Issues require immediate escalation and management notification. No immediate work around available.

Full correction of the application(s) defect shall be completed by Contractor unless otherwise approved by <AGENCY>, and corrections shall be captured as operational improvement lessons. Where necessary, the Contractor shall timely document and instruct its personnel in corrective actions.

Services include updating all appropriate documentation. Additionally, the Contractor shall provide monthly reports showing the amount of warranty work (number of defects and hours to correct, and impact to extended work week/time).

## Policies, Procedures and Standards

### Standards and Common Practices

The following standards will be followed, as applicable to the specific tasks for which they are intended. [Expand list, Examples shown]

* Section 508 Standards (www.section508.gov) IT Security Policies
* OMB Circulars: A-11, Part 7, Planning, Budgeting, and Acquisition of Capital Assets; A- 109, Major Systems Acquisitions; A-123, Management Accountability and Control; A- 127, Financial Management Systems; and A-130, Management of Federal Information Resources National Institute of Standards and Technology (NIST) 800-37 Guidelines for the Security Certification and Accreditation of Federal Information Technology Systems

### After Hours Production Changes

<AGENCY> requires changes to critical systems be done after core/prime hours of service. This requires production changes be done as a 2nd or 3rd shift. Where such ‘after hour’ changes are required the Contractor shall work to maximize the efficiency of its staff or add additional staff for such activities. Where additional staff is added, the Contractor shall develop a process for controlling the handoff of planned changes and establish mechanisms for testing before such changes are made live in the Production environment.

### After Hours Support and Emergency Requirements

Services critical to sustaining server operations may require routine support and ad hoc support outside of the core service hours. As required by the COR, the Contractor shall staff to fill after hour needs, and when it is necessary, the Contractor shall respond to unscheduled problems during non-core service hours. For unplanned, after-hours support, the Contractor shall:

1. Acknowledge initial contact via email/telephone within 15 minutes. Off-hours contact will be via mobile devices (i.e., blackberry, phone, or pager).
2. Respond to emergencies or other activities that require the performance of services outside of the standard service hours.
3. Respond on-site within two (2) hours of initial contact, as necessary.
4. Support Software maintenance releases

### Access to Government Facilities

The Government has the right to restrict and control access to its facilities, property, and data, including those that are identified in this SOW. Access privileges will be tailored to individual Contractor personnel responsibilities. The Government will be the final authority in determining access privileges. The Government’s exercise of its right to grant and revoke the access of particular individual(s) to its facilities, or parts thereof, shall not constitute a breach or change to the Contract, regardless of whether said individual(s) are employed by the Contractor, and regardless of whether said individual(s) are precluded from performing work under the resulting Contract.

### Records Maintenance and Reporting

The Contractor shall create and maintain files (e.g., records, reports, and logs) documenting the processing of work and associated information. Federal laws, regulations, and the direction of the COTR shall govern access to this information.

1. The Contractor shall make files available to the COTR upon request within five (5) business days of receipt of the request. The Contractor shall maintain all records including files, documents, and working papers provided by the Government and/or generated for the Government in the performance of this SOW. These records shall be maintained in a format approved by the COTR. In the event of default, or non-performance, the Government will have immediate access to records in order to ensure mission support is not interrupted. All such records shall be checked into the Government documentation management tool, properly versioned and turned over to the Government at the completion or termination of the Contract.
2. The Contractor shall respond to requests from the COTR for information, including scheduled (programmed) and ad hoc (non-programmed) requests. The Contractor shall refer all requests for support to the COTR if received from other Government personnel prior to responding. The Contractor shall submit to the COTR programmed and un-programmed information.
3. Upon notification by the COTR, the Contractor shall provide management and technical information including, but not limited to, technical evaluation of suggestions and/or alternatives, fact sheets, audits, Congressional inquiries, one-time reports, materials, equipment, facilities, property inventories and other listings, and equipment maintenance records.
4. All records, files, reports, and data deemed proprietary by the Contractor shall be marked accordingly. The Government will make the final determination of the appropriateness of proprietary claims by the Contractor.

## Facilities

The division of support responsibilities between the Contractor and the Government with respect to the provision of all necessary facilities, resources (e.g., hardware/software/network components) and support, for its teams to perform the solution engineering and support services at all Service locations, including on-site and off-site locations. <AGENCY> will provide facilities for housing datacenter and network infrastructure. End users will be located within Government facilities, remote locations, or at employee locations used in official or approved as in performance of Government work (e.g., home office, travel, other Government facilities).

1. Where Contractor facilities are used, the Contractor shall at all times, secure, protect and maintain physical and logical segregation of Government materials, information, and work products from personnel not authorized to perform work activities under the contract/task order. Additionally, the Contractor shall maintain a service continuity support plan ensuring that work activities and contractual responsibilities can be met (e.g., with respect to Contractor owned or leased facilities where services are to be performed, documentation and evidence of service recovery plans, that includes provisions for backup facilities, utilities, staffing, telecommunications, etc.).
2. Where Contractor facilities are used the Contractor shall be technical and financially responsible for the connections between the Contractor’s facility(ies) and Government locations.
3. The Contractor shall attain certification and maintain an Authority to Operate. The Contractor shall, at all times, comply with all FISMA requirements and standards issued by the National Institute of Standards and Technology (NIST).

## Operations and Maintenance

### Data Center

The majority of the systems maintained by the infrastructure support groups are located within

<AGENCY>’s secured Data Center. The data center is staffed 24-hours/day, seven-days/week, and is a controlled environment for the resources and also acts as the focal point for system monitoring, and customer services.

The Data Center is comprised of both virtual and physical Unix servers supporting the Corporate Applications Service Area. Other equipment includes (but is not limited to) Physical and virtual Microsoft Windows servers, Cisco routers, switches, security appliances and Wireless Access Points that support the Network Service Area. The Data Center is cabled under raised floor in a 7,400 square foot-controlled environment facility. The routers, switches, and appliances are distributed in the datacenter and in 23 separate Communication Equipment Rooms (CERs) on the floors of <AGENCY>’s two Headquarters buildings.

The Operations Team performs the following tasks that include (but are not limited to:) (see Appendix XXX).

* + - * Providing an environment with reliable conditions for temperature, humidity
			* Housing of servers and the logistical activities
			* Hosting of servers and storage systems including operating-system support and basic database administration
			* Backup and restore services
			* Monitoring of infrastructure services as local area network and external communications (except conventional telephone service (POT))
			* Monitoring of infrastructure applications like email-services including spam filters, virus protection, fax servers, Domain Name Services (DNS), LDAP- and other directory services
			* Monitoring of off-site (hosted) applications and services (e.g. cloud email, backup, hosted systems)
			* Inventory validation
			* Physical equipment management
			* Event management of reported service outages and management escalation
			* Change control

Through round-the-clock monitoring, the Operations Team manage the central servers, and other configured services to ensure that systems are working at all times (except during scheduled outages).

The Operations Team also provides offsite storage for electronic data and hardcopy back-up records. System backups are sent offsite to protect from fire or other destructive events within the computer facility.

Table – Data Center Roles and Responsiblities

| **Data Center Roles and Responsibilities** | **Provider** | **<AGENCY>** |
| --- | --- | --- |
| 1. Financial responsibility for Infrastructure and assets
 | No | Yes |
| 1. Architectural decisions and asset refresh
 | No | Yes |
| 1. Provide facility and Data Center-related environmental elements (e.g., HVAC, dual redundant UPS, power, cable plant, fire detection and suppression systems, temperature, and humidity controls, and controlled physical access with 24×7 manned security).
 | No | Yes |
| 1. Manage event and workload processes across all platforms.
 | Yes | No |
| 1. Provide technical support for all hardware/equipment of the Data Center computing infrastructure (see Appendix C10).
 | Yes | No |
| 1. Provide liaison support to all <AGENCY> maintenance contracts and are the point of contact for restoration of services.
 | Yes | No |
| 1. Support Data Center Infrastructure System Software (e.g., operating systems, utilities, databases, Active Directory, Microsoft Office 365, Instant Messaging, SharePoint, DHCP, DNS, Middleware see Appendix C15), local and wide area network monitoring.
 | Yes | No |
| 1. Monitor Data Center Networks (e.g., LAN, WAN connection) and related operations (e.g., systems monitoring, Incident diagnostics troubleshooting, resolution and escalation,) as required to meet <AGENCY> computing requirements.
 | Yes | No |
| 1. Monitor Storage Area Networks, Fiber Channel Infrastructure, and related operations (e.g., systems monitoring, incident diagnostics, troubleshooting, resolution and escalation, -) as required to meet <AGENCY> computing requirements.
 | Yes | No |
| 1. Manage, support and report Back up Services and related operations (e.g., desktop and server) as required to meet <AGENCY> computing requirements.
 | Yes | No |
| 1. Provide coordination that supports agency applications test-to- production deployment/migration activities.
 | Yes | No |
| 1. Implement and coordinate all changes to the Data Center infrastructure including those that may affect the Service Levels of any DIS- implemented and 3rd Party systems managed by the operations team.
 | Yes | No |
| **Monitoring Operations Roles and Responsibilities** | **Empty Cell** | **Empty Cell** |
| 1. Define monitoring requirements and policies.
 | No | Yes |
| 1. Monitor systems and network availability/performance on a 24/7 seven day a week basis.
 | Yes | No |
| 1. Develop and document ”run books” that detail monitoring procedures needed to meet mandated requirements and adhere to defined internal policies
 | Yes | No |
| 1. Review and approve monitoring procedures.
 | No | Yes |
| 1. Identify and report problems that include (but are not limited to:) system, file, disk, and application Problems.
 | Yes | No |
| 1. Provide troubleshooting, repair or escalation of problems that occur in the Data Center computing environment or are reported to the Data Center staff.
 | Yes | No |
| **Production Changes** | **Empty Cell** | **Empty Cell** |
| 1. Define schedule and approve all changes.
 | No | Yes |
| 1. Perform scheduled changes to production servers after core hours.
 | Yes | No |
| 1. Implement and manage scheduling tools for managing/automating job execution (e.g., job workflow processes, interdependencies).
 | Yes | No |
| 1. Perform approved changes to all non-production environments as needed.
 | Yes | No |

### Network

Most of <AGENCY>’s central and personal computer applications and files are accessed via <AGENCY>-managed workstations over <AGENCY>’s centrally maintained Internal (wired) Network. In addition, <AGENCY> maintains an External (wired and wireless) Network to provide Internet connectivity for visitors (e.g., panelists). This network supports a significant portion of approximately twenty thousand visitors <AGENCY> receives annually. Due to the increased use of laptops and mobile devices, <AGENCY> is currently in the process of establishing a secure wireless network for the use of staff and associates. Finally, <AGENCY> maintains the High-Speed network that is physically separated from all other production networks and is used for research purposes only.

Network file, print, application, database, and utility servers are located in the <AGENCY> Data Center. Network devices (e.g., routers, switches) are located in the <AGENCY> Data Center and in Communications Equipment Rooms located on the floors of <AGENCY>’s two Headquarters buildings, which are adjacent and essentially cabled as one building.

<AGENCY> has a single, critical service 1 GB Ethernet circuit connection to the Internet (diverse paths and service centers) and another 1 GB Ethernet connection to Internet2 for the High-Speed network. Regarding wide area connectivity, <AGENCY> maintains one 1 GB Ethernet circuit to an offsite data center to accommodate backup requirements and a T1 point- to-point circuit to another federal government agency. <AGENCY> requires all documents to have current plus three previous versions.

Table – Network LAN/WAN Roles and Responsiblities

| **Network LAN/WAN Roles and Responsibilities** | **Provider** | **<AGENCY>** |
| --- | --- | --- |
| 1. Define and spec WAN/LAN/VPN/Firewall requirements including internal/external and wired/wireless networks.
 | No | Yes |
| 1. Review and approve implementation of WAN/LAN/VPN/Firewall products.
 | No | Yes |
| 1. Define and audit services and standards for all network services.
 | No | Yes |
| 1. Document and Maintain all WAN/LAN/VPN/Firewall infrastructure including internal/external and wired/wireless networks.
 | Yes | No |
| 1. Document and Maintain Trusted Internet Connection (TIC) provided as MTIPS Networx circuit.
 | Yes | No |
| 1. Document and Maintain Content Filtering system on the High-Speed network.
 | Yes | No |
| 1. Document and Maintain Network Access Control (NAC) system (802.1x).
 | Yes | No |
| 1. Perform network liaison function with 3rd parties and operational units such as the Networx provider.
 | Yes | No |
| 1. Monitor and Report network capacity thresholds and recommended improvements with lead time to implement the solution.
 | Yes | No |
| 1. Approve proposed network capacity thresholds and improvements.
 | No | Yes |
| 1. Provide capacity and performance reports including the following( but is not limited to) Response times, Throughputs, Peaks, and averages on a daily, monthly, quarterly basis.
 | Yes | No |
| 1. Procure/Provision all network components and circuits.
 | No | Yes |
| 1. Report performance against service-level requirements as defined by <AGENCY>.
 | Yes | No |

### Design/Engineering

The following identifies the activities, roles and responsibilities associated with Network Engineering/Development services that are specific to this schedule.

Table – Engineering/Development Roles and Responsiblities

| **Engineering/Development Roles and Responsibilities** | **Provider** | **<AGENCY>** |
| --- | --- | --- |
| 1. Develop, maintain, and document network design, engineering and security testing and integration procedures that meet requirements and adhere to defined policies.
 | Yes | No |
| 1. Approve network design engineering, security testing and integration procedures.
 | No | Yes |
| 1. Prepare and deliver to <AGENCY> for approval network design, engineering, security, plans and schedules to support new and enhanced applications, architectures, and standards.
 | Yes | No |
| 1. Review and approve network design, engineering and security plans and schedules.
 | No | Yes |
| 1. Approve the scheduling of all changes to the network environment.
 | No | Yes |
| 1. Coordinate actions with <AGENCY>, affiliated entities, and public carriers.
 | Yes | No |

### Implementation Services

The following identifies the activities, roles and responsibilities associated with Implementation services that are specific to this schedule.

Table – Implementation Services Roles and Responsiblities

| **Implementation Services Roles and Responsibilities** | **Provider** | **<AGENCY>** |
| --- | --- | --- |
| 1. Allocate provider resources with <AGENCY> vendors and other <AGENCY> Contractors to implement the approved Engineered solutions.
 | Yes | No |
| 1. Approve implementation schedules and plans.
 | No | Yes |
| 1. Implement the approved solutions.
 | Yes | No |
| 1. Review and verify implemented solution meets <AGENCY> requirements.
 | No | Yes |
| 1. Provide a Post Implementation review of the implemented changes within 2 weeks of any completed solutions.
 | No | Yes |

### Operations and Administration

The following table identifies the activities, roles and responsibilities associated with Network Operations and Administration that are specific to this Schedule.

1. Operations activities include:
2. Network systems management and troubleshooting (e.g., performance, problem, change and capacity monitoring).
3. Bandwidth management and trending analysis.
4. Protocol usage statistics (e.g., identify top talkers by protocol).
5. Working with public carriers and other circuit providers to perform any operations or maintenance activities (e.g., provisioning, problem management).
6. Managing and maintaining all Network Service computing resources (e.g., hardware, operating system software and applications) that are required to provide Designated Services.
7. Manage version control and ensure all network devices are up to date and fully patched as per manufacturer’s guidelines.
8. Administration services include activities, such as:
9. Managing router configurations, firewalls, Internet Protocol (IP) addresses and related services (e.g., DNS/DHCP).
10. Asset management, including infrastructure software licenses.
11. Physical (e.g., equipment) and logical (e.g., IP address change) IMACs.
12. Network admission control management and administration.

Table – Operations and Adminstration Roles and Responsiblities

| **Operations and Administration Roles and Responsibilities** | **Provider** | **<AGENCY>** |
| --- | --- | --- |
| 1. Maintain LAN/WAN connectivity contained in the service environment.
 | Yes | No |
| 1. Develop and document network administration CONOPS.
 | Yes | No |
| 1. Develop and document procedures for administration that meet requirements and adhere to defined policies and procedures.
 | Yes | No |
| 1. Approve administration CONOPS and procedures.
 | No | Yes |
| 1. Perform day-to-day network operations and administration activities.
 | Yes | No |
| 1. Manage all network devices in accordance with <AGENCY>’s policies (including security oversight and change management policies).
 | Yes | No |
| 1. Maintain IP addressing schemes, router configurations, routing tables, VPN configurations, etc.
 | Yes | No |
| 1. Manage user accounts as needed for access and maintaining network resources (e.g., logon user-id and password maintenance).
 | Yes | No |
| 1. Maintain and provide audit information including access, general logs, application logs in accordance with <AGENCY>’s security policies.
 | Yes | No |
| 1. Ensure that network administration activities are coordinated through <AGENCY> defined change management processes.
 | Yes | No |
| 1. Ensure all network devices are the current version per manufacturer’s guidelines and government approval.
 | Yes | No |
| 1. Notify government at least 1 year ahead of devices that are approaching end of life or end of manufacturer support.
 | Yes | No |
| 1. Acquisition of replacement equipment or service support contracts.
 | No | Yes |

### Monitoring and Reporting

The following table identifies the roles and responsibilities associated with Network Monitoring and Reporting services that are specific to this Schedule.

Table – Network Montioring and Reporting Roles and Responsiblities

| **Network Monitoring and Reporting Roles and Responsibilities** | **Provider** | **<AGENCY>** |
| --- | --- | --- |
| 1. Develop and revise requirements and policies for network monitoring and problem management as needed.
 | No | Yes |
| 1. Document and perform practices for network monitoring and problem management.
 | Yes | No |
| 1. Document and perform network monitoring and problem management procedures, including escalation thresholds, that meet requirements and adhere to defined policies.
 | Yes | No |
| 1. Approve network monitoring and problem management procedures.
 | No | Yes |
| 1. Provide and implement tools for monitoring network devices and traffic.
 | Yes | No |
| 1. Implement measures for proactive monitoring and self-healing capabilities to limit network outages.
 | Yes | No |
| 1. Monitor network for, and report, failures with Service Levels.
 | Yes | No |
| 1. Identify network problems and resolve in accordance Incident and Problem Management Services, polices, procedures.
 | Yes | No |
| 1. Provide on-site staff at <AGENCY> facilities as required to perform maintenance and problem resolution activities.
 | Yes | No |
| 1. Coordinate resolution of circuit problems with third parties, including public carriers, ISP, and affiliates.
 | Yes | No |

### Documentation

The following are required document types that are specific to this Schedule.

1. Network system specifications and topologies (for example, router configurations, firewall policies, routing diagrams/IP addressing tables, hardware/software listings, etc.)
2. Detailed circuit location information (e.g., circuit ID including LEC access ID, and location)
3. Detailed documentation showing all firewall policy, group, object, etc. information
4. “As-built” documentation for all network devices (including firewalls) that are deployed in development, test, QA, production, or other technical environments

The following table identifies the roles and responsibilities associated with Documentation activities that are specific to this Schedule.

Table – Documentation Roles and Responsiblities

| **Documentation Roles and Responsibilities** | **Provider** | **<AGENCY>** |
| --- | --- | --- |
| 1. Recommend documentation requirements.
 | Yes | No |
| 1. Define and establish documentation requirements.
 | No | Yes |
| 1. Develop, provide, library documentation as required by <AGENCY>.
 | Yes | No |

## Phone/Voice Support

<AGENCY>’s voice system is comprised of a government furnished Siemens Hicom 300E PBX and associated hardware and software, supporting approximately 2600 telephone sets (mostly digital with some analog for fax). Voice mail is provided through the Siemens Xpressions Messaging System, a unified messaging system that, in addition to providing traditional voice mail services via the telephone, integrates with the <AGENCY> email system to provide access to voice mail messages in Outlook. The Siemens Automated Call Distribution (ACD) system HiPath ProCenter (HPPC) Enterprise supports IT Help Central, <AGENCY>’s IT Help Desk.

Hicom Business View Composer and Observer ACD software provides limited ACD services for some other groups within <AGENCY> and provides backup ACD support to IT Help Central should HPPC be unavailable.

he Contractor is responsible for planning and performing upgrades and patching of Xpressions, HPPC, and Business View ACD to ensure vendor support and product compatibility with other products. The phone system, the Xpressions system, and the ProCenter system are on an APC Matrix UPS system providing 8 hours of battery backup.

### Desk Phone Service

Provider will support <AGENCY> telephone services to employees throughout <AGENCY> facilities. Services include moves, adds and changes (MAC), user training and monitoring and management of the telephone services.

Table – Desk Phone Service Roles and Responsiblities

| **Desk Phone Service Roles and Responsibilities** | **Provider** | **<AGENCY>** |
| --- | --- | --- |
| 1. Provide Desk Phone requirements (e.g., number of sets, functions, and features).
 | No | Yes |
| 1. Perform Desk Phone support, moves, adds, changes, administration, and troubleshooting.
 | Yes | No |
| 1. Approve changes to Desk Phone design and engineering.
 | No | Yes |
| 1. Provide end to end internal and external phone connectivity including activities for connecting hardware and/or peripherals.
 | Yes | No |
| 1. Configure Desk Phone for services (e.g., Emergency 911).
 | Yes | No |
| 1. Perform setup and training for adaptive voice telecommunications services and equipment as required by laws affecting the support of the disabled.
 | Yes | No |

### Telecommunications (Network, Conferencing and Voice) Services

The <AGENCY> currently uses the GSA Networx, WITS3 (Washington Interagency Telecommunications System), and other GSA contracts to provide Telecommunications services to <AGENCY> users. These contracts include Network (Trusted Internet Connection, data services, Conferencing (video, voice, web) and Voice services (long distance, local, calling card, toll-free) services. The provider will support, monitor, and manage the Telecommunications services provided by these contracts and delivery to <AGENCY> users.

Table – Voice Network Services Roles and Responsiblities

| **Long Distance Services Roles and Responsibilities** | **Provider** | **<AGENCY>** |
| --- | --- | --- |
| 1. Provide Telecommunications Services strategies and requirements
 | No | Yes |
| 1. Provide Telecommunications Services design and engineering to meet <AGENCY> strategies and requirements
 | Yes | No |
| 1. Approve Telecommunications Services design and engineering
 | No | Yes |
| 1. Support, monitor, manage Telecommunications Services (TIC, data, web, video, voice conferencing, long distance, local, calling card, toll- free)
 | Yes | No |
| 1. Provision individual conferencing services (video, voice, web) and long- distance calling cards and manage/report use to <AGENCY> per <AGENCY> policies
 | Yes | No |
| 1. Provide Network, Conferencing, and Voice services usage monitoring and reporting
 | Yes | No |

### Voice Messaging

Provider shall provide Voice Messaging services to allow the efficient exchange of messages between two or many people enterprise wide. The following table identifies the roles and responsibilities associated with Voice Messaging services.

Table – Voice Messaging Services Roles and Responsibilities

| **Voice Messaging Roles and Responsibilities** | **Provider** | **<AGENCY>** |
| --- | --- | --- |
| 1. Provide Voice Messaging Services strategies and requirements.
 | No | Yes |
| 1. Provide Voice Messaging Services design and engineering to meet <AGENCY> strategies and requirements.
 | Yes | No |
| 1. Approve Voice Messaging Services design and engineering changes.
 | No | Yes |
| 1. Configure and support Voice Messaging Services.
 | Yes | No |
| 1. Monitor and report Voice Messaging usage statistics.
 | Yes | No |
| 1. Monitor and report Voice Messaging storage capacity usage statistics.
 | Yes | No |
| 1. Support <AGENCY> Voice Messaging retention requirements and regulations.
 | Yes | No |
| 1. Perform mailbox moves, adds and changes.
 | Yes | No |
| 1. Maintain mailbox configurations by user.
 | Yes | No |
| 1. Provide user guide to new users and instruction where needed.
 | Yes | No |

### Contact Center Service

Provider shall provide Contact Center Service that provides Toll-free call processing and call flow with integrated ACD, IVR, CMS, and future CTI support and CRM integration. Services include planning and assessment, implementation, and ongoing management necessary to deploy Contact Center Services enterprise wide. The following table identifies roles and responsibilities associated Contact Center Service activities.

Table – Contract Center Service Roles and Responsiblities

| **Contact Center Services Roles and Responsibilities** | **Provider** | **<AGENCY>** |
| --- | --- | --- |
| 1. Provide Contact Center Services strategies and requirements.
 | No | Yes |
| 1. Recommend Contact Center Services to meet <AGENCY> strategies and requirements.
 | Yes | No |
| 1. Approve Contact Center Services.
 | No | Yes |
| 1. Provision and or configure Contact Center Services.
 | Yes | No |
| 1. Provide Inbound Toll-Free Number.
 | No | Yes |
| 1. Manage Inbound Toll-Free Services.
 | Yes | No |
| 1. Provide administrative support for Inbound Toll-Free services.
 | Yes | No |
| 1. Coordinate with internal customers and external carriers to fulfill requests concerning toll-free services including new orders, cancellations, Moves, Adds and Changes (MACs).
 | Yes | No |
| 1. Design and implement customized call flow.
 | No | Yes |
| 1. Perform agent/queue moves, adds, and changes, including desktop connectivity.
 | Yes | No |
| 1. Provide consultation to contact center owners in developing new or modifying existing ACD applications.
 | Yes | No |
| 1. Provide traffic analysis and call reports for all requested metrics such as:800 in-bound network traffic, call detail, trunk utilization, etc.
 | Yes | No |
| 1. Monitor and maintain IVR functionality, host, and PBX connectivity.
 | Yes | No |
| 1. Provide IVR reports on system, network, and application availability.
 | Yes | No |
| 1. Generate call volume trend report for all applications including weekly call volumes for decodes, accounts payable and expense reports.
 | Yes | No |
| 1. Provide and maintain monthly reports of all IVR status including hardware (spare, in-use) critical parts, software, interfaces, and scripts by Business Unit.
 | Yes | No |
| 1. Provide an attempted (offered) and handled call volume summary.
 | Yes | No |
| 1. Provide duration, call transferred and abandoned call reports.
 | Yes | No |
| 1. Provide weekly line usage reports with call volume by port number.
 | Yes | No |

## Enterprise Services

### Directory Service

Offeror shall provide Directory Services to support the internal-facing directory. <AGENCY>’s internal directory is based on Microsoft Active Directory and its main purpose is to provide network authentication along with all associated systems such as SharePoint, Exchange, etc. The following table identifies the roles and responsibilities associated with Directory Services activities.

Table – Directory Services Roles and Responsibilities

| **Directory Services Roles and Responsibilities** | **Provider** | **<AGENCY>** |
| --- | --- | --- |
| 1. Provide Directory Services strategies and requirements.
 | No | Yes |
| 1. Provide recommendations to meet <AGENCY> strategies and requirements.
 | Yes | No |
| 1. Approve Directory Services recommendations.
 | No | Yes |
| 1. Provide a secure and searchable online directory service with real time updates.
 | Yes | No |
| 1. Manage content and access (e.g., directories) on <AGENCY> Intranet.
 | Yes | No |
| 1. Provide administrative support for Online Directory services to maintain and update the directory in accordance with agreed upon service levels.
 | Yes | No |
| 1. Perform monthly audits of online directory for employee, Contractor, and vendors to ensure data integrity.
 | Yes | No |

### Identity Management

<AGENCY> has implemented an Identity Management (IDM) solution to reduce the number of passwords a user must remember and maintain as a part of Corporate Directory services.

Identity Management relies upon the Oracle Identity Manager product suite. It is also integrated with Windows Active Directory.

Table – Identity Management Roles and Responsibilities

| **Identity Management Roles and Responsibilities** | **Provider** | **<AGENCY>** |
| --- | --- | --- |
| 1. Develop requirements and policies for Identity Management.
 | No | Yes |
| 1. Document and perform activities.
 | Yes | No |
| 1. Resolve problem management issues.
 | No | Yes |
| 1. Maintain configuration and manage Identity Management with <AGENCY> supplied tools.
 | Yes | No |

### Remote Access

Secure remote access to most applications is available using Access <AGENCY> (a VPN- based service), Access Workspace (a Citrix-based service) and Outlook Web Access (OWA), all secured using SecurID tokens and two-factor authentication. Blackberries and other PDAs such as iPhones and iPads are also supported. <AGENCY> is moving towards full compliance with HSPD-12, where the PIV card will provide 2-factor authentication and eventually move away from token and passwords.

Table – Remote Access Roles and Responsiblities

| **Remote Access Roles and Responsibilities** | **Provider** | **<AGENCY>** |
| --- | --- | --- |
| 1. Define Remote Access policies and procedures
 | No | Yes |
| 1. Develop and document in the Standards and Procedures Manual Remote Access procedures that meet requirements and adhere to defined policies
 | Yes | No |
| 1. Review and approve Remote Access procedures
 | No | Yes |
| 1. Install, test, provide technical support, administration and security administration for Remote Access hardware and Software
 | Yes | No |
| 1. Provide testing support for defined <AGENCY> applications that will be made available via Remote Access
 | Yes | No |
| 1. Provide technical assistance and subject matter expertise as required by <AGENCY> staff and 3rd party solution providers for Remote Access products and solutions
 | Yes | No |
| 1. Perform system or component configuration Changes necessary to support Remote Access Services
 | Yes | No |

### Desktop Management

<AGENCY> Desktop Management activities follow:

* + - * Desktop hardware and desktop software. This includes hardware imaging and maintenance of <AGENCY>’s standard images. In this case, the term “desktop” includes workstations, laptops, PDAs, and other mobile devices.
			* Services provided via network administration. This includes centralized configuration management such as application patching, update, and rollout; maintenance of the Microsoft Office Active Directory Group Policy; and management of the Federal Desktop Core Configuration. Current configuration management tools include Windows Server Update Services (WSUS), Radia and Shavlik.
			* Planning, coordination, and special studies. In addition to planning, this includes integrated change management, requirements definition, new application evaluation and insertion, and establishing desktop performance expectations.

With respect to Desktop Management, <AGENCY>’s IT Help Central will be responsible for executing the Desktop hardware and desktop software task.

Table – Desktop Management Roles and Responsibilities

| **Desktop Management Roles and Responsibilities** | **Provider** | **<AGENCY>** |
| --- | --- | --- |
| 1. Define Desktop/end user business requirements and platform standards and architecture.
 | No | Yes |
| 1. Recommend services and standards for supporting the <AGENCY> desktop/end user business requirements and platform standards.
 | Yes | No |
| 1. Review and approve recommendations for services and standards for supporting the desktop/end users.
 | No | Yes |
| 1. Procure and own desktop and laptop hardware and software.
 | No | Yes |
| 1. Manage logistics and configuration for hardware and software from time of arrival at facility (e.g., checkout, installation, maintenance, disposal).
 | Yes | No |
| 1. Deploy and manage desktop and laptop hardware and software (e.g., operating system, personal productivity and office automation software and services).
 | Yes | No |
| 1. Setup network-attached attached printers, copiers, scanners, and fax devices.
 | Yes | No |
| 1. Provide end-user data back-up, storage, and recovery services.
 | Yes | No |
| 1. Provide and support remote access services for <AGENCY> employees and its client end-users in mobile, remote, and home locations.
 | Yes | No |
| 1. Approve problem determination and resolution for all in-scope devices.
 | No | Yes |
| 1. Provide Level 2 and Level 3 hardware and system software support for all in-scope hardware and software as coordinated through the <AGENCY> Help Desk.
 | Yes | No |
| 1. Coordinate service delivery with the <AGENCY> Help Desk, as well as the Level 2 support groups within each of the other service delivery areas.
 | Yes | No |
| 1. Manage parts and shipments with 3rd parties.
 | Yes | No |

### Core Software Build and Deployment Services

Core Software is defined as the set of components that comprise the suite of software programs used to build an <AGENCY>-defined standard end-user device image, including operating system software, office productivity and messaging software, database software, security tools, remote connectivity software, and remote management and deployment tools. Provider will perform the Core Software Deployment activities associated with the provision of Desktop and End-user Computing infrastructure. The following table identifies Core Software Build and Deployment roles and responsibilities.

Table – Core Software Deployment Roles and Responsiblities

| **Core Software Build and Deployment Roles and Responsibilities** | **Provider** | **<AGENCY>** |
| --- | --- | --- |
| 1. Recommend core software deployment/management policies and procedures.
 | Yes | No |
| 1. Review and approve core software deployment/ management policies and procedures.
 | No | Yes |
| 1. Specify Core Software platform architectural requirements for which build and deployment services must be provided.
 | No | Yes |
| 1. Provide technical assistance for defining core image(s) specifications for desktops, laptops, and other in-scope end-user computing devices.
 | Yes | No |
| 1. Develop and document detailed technical specifications that define and support the build, test, and deployment plans for the standard core image(s).
 | Yes | No |
| 1. Approve standard core image(s) specifications and deployment plans.
 | No | Yes |
| 1. Build core software end-user device image(s) and provide documentation of results to <AGENCY>.
 | Yes | No |
| 1. Conduct system-level testing of the core software image(s) to validate that they perform in accordance with the approved specifications.
 | Yes | No |
| 1. Perform end-user acceptance testing of the Core Software image(s).
 | No | Yes |
| 1. Approve core software image(s) for release.
 | No | Yes |
| 1. Assist in the end-user testing, as required.
 | Yes | No |
| 1. Coordinate with the <AGENCY> Help Desk, and other support groups as applicable, to ensure that each of the appropriate IT Service groups are prepared to support the deployment of the Core Image(s).
 | Yes | No |
| 1. Provide necessary utilities/tools to maintain and ensure compliance with core software deployment/management policies and procedures.
 | Yes | No |
| 1. Manage deployment efforts using formal project management tools, methodologies, and standards (e.g., ITIL change and configuration management practices).
 | Yes | No |
| 1. Deploy approved core image(s) on all in-scope Desktop and End-user devices.
 | Yes | No |
| 1. Provide, staff, and administer a software distribution facility.
 | Yes | No |
| 1. Recreate end-user desktop environment to previous state including base build plus all end user specific features, functions, and applications.
 | Yes | No |
| 1. Develop scripts and macro programs to automate standard <AGENCY> processes as appropriate (e.g., upgrading desktop images).
 | Yes | No |
| 1. Develop, implement, and maintain macro programs for <AGENCY> standard distributed computing applications and processes.
 | Yes | No |
| 1. Conduct deployment reviews and provide results to <AGENCY>.
 | Yes | No |
| 1. Review and approve results of deployment reviews.
 | No | Yes |

### Helpdesk Services

Helpdesk Services represent that support by the Contractor necessary to managing performance and troubleshooting incidents, answering questions, or resolving issues with server and network operations. The activities and descriptions included are based on industry practices and Contractor support shall align to descriptions used by the Helpdesk Institute.

Services include, but are not limited to the coordination, management, and second level

response to Incidents and Service Requests made by the Helpdesk and <AGENCY> technical staff. <AGENCY> shall be responsible for providing the Contractor with access to the Siebel Helpdesk system. The Contractor is not responsible for Tier I support but shall provide support from the time that a ticket is logged by Tier I and then assume end-to-end ownership (e.g., tracking, Resolution, and reporting) of assigned Help Desk Incidents and Service Requests through use of the Government provided system.

### Incident & Problem Management

Incident and Problem Management includes the activities associated with restoring normal service operation as quickly as possible and minimize the adverse impact on business operations, thus ensuring that the best possible levels of service quality and availability are maintained.

The Contractor shall institute procedures for minimizing the adverse impact of incidents and problems on ITIS that are caused by errors in misuse by users, application errors affecting hardware and software (e.g., Operating System, Utilities, Database, Middleware, etc.) and shall implement actions that prevent the recurrence of Incidents related to those errors. The Contractor shall establish procedures for identifying root cause of incidents and then initiate actions to improve or correct the situation. Where escalation of issues is necessary the Contractor shall provide timely notification of issues – notwithstanding whether issues are within or outside the control of the Contractor – and shall coordinate and participate with the Government PMO in addressing resolutions, changes, or fixes.

The Contractor support shall be provided as follows:

1. *Level 2 Support* – assistance to the ITHCS help desk to analyze incidents or problems, identify root causes, and resolve the incidents or problems if such incidents or problems are identified as minor. If such incidents or problems are identified by the Level 2 Support team as major, such incidents or problems shall be routed to the Level 3 Support team. For Level II Desk-side Support the Contractor shall support user-Level triage of all tickets, prioritization of those forwarded to Tier II (PMO), providing Subject Matter Experts (SMEs) skilled in the particular system and related issues, work with users to address problems, analysis of business processes, system or training problems, and participation with the change control board in proposing changes that will benefit the field or that will make Tier II Support more effective.

For *Level 2 PMO* support the Contractor shall provide Subject Matter Expertise (SMEs) capable of providing the Government PMO with advice and recommendations on improvements to correcting process related issues, working with users to address user problems, analyzing problems, recommending solutions, testing changes, identifying problems with 3rd parties, and recommending changes; and

1. *Level 3 Support* – Level 3 Support shall perform a detailed root cause analysis and assess overall impact with respect to incidents and problems relating to unique issues with hardware and software Infrastructure, databases, interfaces, and connections that cannot be resolved by Level 2. Level 3 Support shall also coordinate with others (e.g., the applications development and maintenance staff, Security, etc.). At Level 3 the Contractor shall provide, but is not limited to providing expertise in developing, testing, implementing, fixes in:
	* Participating in reviews as Technical IPT members
	* Analyzing and recommending enhancements and fixes
	* Performing system maintenance (applications, tables, content, documentation)
	* Testing approved system changes
	* Documenting resolutions and changes

The following table identifies Incident and Problem Management roles and responsibilities associated with Service Support.

Table – Incident and Problem Management Roles and Responsiblitites

| **Incident and Problem Management Roles and Responsibilities** | **Provider** | **<AGENCY>** |
| --- | --- | --- |
| 1. Helpdesk and management tool (Siebel) financial and licenses
 | No | Yes |
| 1. Provide Contractor with access to Siebel.
 | No | Yes |
| 1. Level 2 and Level 3 Support as defined by HDI and by the contract terms and statement of work for technology areas identified.
 | Yes | No |
| 1. Supplemental Support and governance
 | No | Yes |
| 1. Help Desk Ticket coordination and management
 | Yes |  |
| 1. <AGENCY> Incident and Problem management policies
 | No | Yes |
| 1. Compliance with <AGENCY> Incident and Problem management policies and procedures – recommend changes as appropriate
 | Yes | No |
| 1. Establish operations and service management QA and control programs that are consistent with ITIS QA and control policies and processes.
 | Yes | No |
| 1. Approve operations and service management QA and control programs.
 | No | Yes |
| 1. Perform and report Contractor QA and quality control programs.
 | Yes | No |
| 1. Coordinate support activities w/ the ITIS Help Desk – Level I.
 | Yes | No |
| 1. Establish incident/problem classification by Severity Level.
 | No | Yes |
| 1. Establish incident/problem workflow, escalation, communication, and reporting processes that achieve serviced metric requirements.
 | Yes | No |
| 1. Review and approve incident/problem classification, prioritization and workflow, communication, escalation, and reporting processes.
 | No | Yes |
| 1. Configure, and operate incident and problem management processes and data within Siebel.
 | Yes | No |
| 1. Manage details and resolution of assigned ticket for entire incident/problem life cycle including detection, interaction with other support functions (Levels 2 and 3), to diagnose, and report repair and resolution.
 | Yes | No |
| 1. Ensure incident resolution activities conform to defined change control procedures.
 | Yes | No |
| 1. Coordinate handoffs of workflow and incidents back to Level I and coordinate action with 3rd party providers (e.g., vendors, public carriers, ISP).
 | Yes | No |
| 1. Where necessary participate in problem resolution with ITIS and third parties (e.g., public carriers, ISP).
 | Yes | No |
| 1. Perform Contractor Root Cause Analysis of incidents, including engaging ITIS teams as required, document findings and take corrective actions for in scope services. Resolve problem and/or substantiate that all reasonable actions have been taken to prevent future reoccurrence.
 | Yes | No |
| 1. Periodically review the state of open problems and the progress being made in addressing problems.
 | Yes | No |
| 1. Participate in problem review sessions and provide listing and status of problems categorized by problem impact.
 | Yes | No |
| 1. Authorize ticket closure of ITIS initiated tickets.
 | No | Yes |
| 1. Identify possible enhancement opportunities for improved operational performance and potential cost savings.
 | Yes | No |
| 1. Approve projects to implement operational improvements.
 | No | Yes |

### Root Cause Analysis

Contractor shall develop, implement, and maintain a Root Cause Analysis (RCA) process and perform the activities required to diagnose, analyze, recommend, and take corrective measures to prevent recurring problems and/or trends. The following table identifies RCA roles and responsibilities associated with Service Support.

Table – Root Cause Analysis Roles and Responsiblities

| **Root Cause Analysis (RCA) Roles and Responsibilities** | **Provider** | **<AGENCY>** |
| --- | --- | --- |
| 1. Identify requirements and policies for Root Cause Analysis (e.g., events that trigger an RCA).
 | No | Yes |
| 1. Follow existing procedures for performing an RCA that meet requirements and adhere to defined policies – recommend changes as appropriate.
 | Yes | No |
| 1. Approve RCA procedures.
 | No | Yes |
| 1. Engage other non-Contractor resources in RCA.
 | No | Yes |
| 1. Conduct proactive trend analysis to identify recurring problems.
 | Yes | No |
| 1. Track and report recurring problems or failures and provide associated consequences of problems if there is a business impact to ITIS.
 | Yes | No |
| 1. Recommend solutions to address recurring problems or failures.
 | Yes | No |
| 1. Approve solutions to address recurring problems or failures.
 | No | Yes |
| 1. Flag and track until closure all incidents that require RCA.
 | Yes | No |
| 1. Identify root cause of incidents and recommend appropriate resolution action.
 | Yes | No |
| 1. Approve solutions to address incidents and prevent recurrence.
 | No | Yes |
| 1. Provide status report detailing the root cause of and procedure for correcting recurring problems.
 | Yes | No |

## Business Systems

<AGENCY>’s systems that support grants management, the main mission of the organization, are primarily Java based using Weblogic and Glassfish. These application and web servers are primarily Oracle Solaris operating systems. The following table delineates some of the provider’s main responsibilities:

Table – Data Management Roles and Responsibilities

| **Data Management Roles and Responsibilities** | **Provider** | **<AGENCY>** |
| --- | --- | --- |
| 1. Perform system administration to ensure service level agreements and according to <AGENCY> policies and regulations.
 | Yes | No |
| 1. Deploy new applications and/or releases according to standard operating procedures.
 | Yes | No |
| 1. Provide new code and development of business applications.
 | No | Yes |
| 1. Maintain data storage assets (e.g., RAID array, SAN, NAS, tape, optical, etc.) through direct support or through 3rd party services (e.g., warranty and maintenance) as approved by <AGENCY>.
 | Yes | No |
| 1. Coordinate 3rd party activities for repair or installation when 3rd party agreements are used or devices are under warranty.
 | Yes | No |
| 1. Install patches and service packs within 60 days of release.
 | Yes | No |

### Database Management

<AGENCY>’s internally developed central applications are based mainly on Sybase databases residing on Sun Microsystems equipment running Solaris Operating System. Microsoft SQL Server supports Commercial Off-The-Shelf (COTS) products (e.g., Siebel, Radia, Shavlik, etc.) and is based primarily on servers running Microsoft Windows Operating System. Research.gov runs on Oracle.

The Contractor’s responsibility is to maintain assets used in data storage and to provide support to database administrators and application owners.

Table – Data Management Roles and Responsiblities

| **Data Management Roles and Responsibilities** | **Provider** | **<AGENCY>** |
| --- | --- | --- |
| 1. Recommend Provider-standard Storage and Data Management procedures.
 | Yes | No |
| 1. Develop, document, and maintain in the Standards and Procedures Manual Storage and Data Management Provider procedures that meet <AGENCY> requirements and adhere to <AGENCY> policies.
 | Yes | No |
| 1. Review, provide additional procedures as required and approve Storage and Data Management procedures.
 | No | Yes |
| 1. Monitor and control storage performance according to technical Specifications, Storage and Data Management policies, and perform tuning as required.
 | Yes | No |
| 1. Maintain and improve storage resource efficiency.
 | Yes | No |
| 1. Maintain data set placement and manage data catalogs.
 | Yes | No |
| 1. Perform data and file backups and restores per established procedures and SLRs.
 | Yes | No |
| 1. Manage file transfers and other data movement activities.
 | Yes | No |
| 1. Provide input processing, for activities such as loading 3rd party media (e.g., tape) and receipt and/or transmission of batch files.
 | Yes | No |
| 1. Acquire and manage consumables, such as tape, disks, etc., in support of the backup requirements. Coordinate acquisition of additional materials as needed.
 | Yes | No |
| **Media Operations Roles and Responsibilities** | **Empty Cell** | **Empty Cell** |
| 1. Recommend Provider-standard Media Operations procedures.
 | Yes | No |
| 1. Develop, document, and maintain in the Standards and Procedures Manual Media Operations Provider procedures that meet <AGENCY> requirements and adhere to <AGENCY> policies.
 | Yes | No |
| 1. Review, provide additional procedures as required and approve media processing procedures.
 | No | Yes |
| 1. Maintain a media library and media management system.
 | Yes | No |
| 1. Manage the media inventory to ensure that adequate media resources are available. Coordinate acquisition of additional media as needed.
 | Yes | No |
| 1. Manage input media availability to meet processing SLRs.
 | Yes | No |
| 1. Load and manage Third media.
 | Yes | No |
| 1. Provide secure off-site storage for designated media and transport media to <AGENCY> approved off-site location as required.
 | Yes | No |
| 1. Perform periodic audits to ensure proper cataloging of media.
 | Yes | No |

### Service Recovery

National Security Presidential Directive/NSPD-51 and Homeland Security Presidential Directive/HSPD-20, dated May 9, 2007, require that all Federal departments and agencies have a Continuity of Operations Plan (COOP). As part of the COOP, the National Science Foundation (<AGENCY>) has a requirement for a comprehensive IT Disaster Recovery Plan (DRP) to restore end-user, communications, system and data center operations for essential government functions and ongoing organizational direction during emergency situations. The DRP is required to be tested regularly in order to update and improve the overall plan.

A DRP will be provided for all <AGENCY> Major Application (MA) Systems, and General Support Systems (GSS), as defined under FISMA (Federal Information Security Management Act).

The <AGENCY> Major Applications (MA) are currently a combination of Client/Server, and Web-based Custom-developed corporate applications using two/three-tiered server architecture hosted on Oracle Solaris (UNIX) and MS Windows servers. <AGENCY>’s mission-related data are stored mainly on Sybase and Oracle databases. Microsoft SQL Server supports smaller databases.

The <AGENCY> General Support Systems (GSS) include LAN and Windows/Unix servers and additional hardware such as SANs, tape and disk backup systems, remote access, and other appliance HW, switches, routers, firewalls, personal computers, and printers.

<AGENCY> has two (2) redundant 1GB connections to the Internet. Remote access to

<AGENCY> MAs is available from the Internet by two-factor VPN connection using RSA SecurID tokens.

#### IT Service Continuity and Service Recovery Services

The Contractor must demonstrate that it will consistently meet or exceed <AGENCY> IT continuity and service recovery requirements and shall comply with any federal requirements on Continuity and Disaster Recovery (DR). The following table identifies IT Service Continuity and Service Recovery Services roles and responsibilities associated with Service Delivery.

Table - IT Service Continuity and Service Recovery Roles and Responsibilities

| **IT Service Continuity and Service Recovery Roles and Responsibilities** | **Provider** | **<AGENCY>** |
| --- | --- | --- |
| 1. Define <AGENCY> IT service continuity and service recovery strategy, requirements, and scenarios.
 | No | Yes |
| 1. Recommend best practice IT service continuity and service recovery strategies, policies, and procedures.
 | Yes | No |
| 1. As needed, assist <AGENCY> in other IT continuity and emergency management activities.
 | Yes | No |
| 1. Assign System Classification for purposes of continuity directives.
 | No | Yes |
| 1. Develop and maintain a detailed <AGENCY> plan to achieve <AGENCY> requirements. Plan shall include plans for data, back-ups, storage management, and contingency operations that provides for recovering <AGENCY>’s systems within established recovery requirement timeframes after a disaster affects <AGENCY>’s use of the Services.
 | No | Yes |
| 1. Define data (e.g., File System, Database, Flat Files) replication, backup, and retention requirements.
 | No | Yes |
| 1. Establish processes to ensure <AGENCY> plans are kept up to date and reflect changes in <AGENCY> environment.
 | No | Yes |
| 1. Review & Approve <AGENCY> plan.
 | No | Yes |
| 1. Establish <AGENCY> test requirements.
 | No | Yes |
| 1. Perform scheduled <AGENCY> tests per <AGENCY> policies.
 | Yes | No |
| 1. Coordinate involvement of users for <AGENCY> testing.
 | No | Yes |
| 1. Participate in <AGENCY> tests.
 | Yes | No |
| 1. Track and report <AGENCY> test results to <AGENCY>.
 | Yes | No |
| 1. Review & approve <AGENCY> testing results.
 | No | Yes |
| 1. Develop action plan to address <AGENCY> testing results.
 | Yes | No |
| 1. Approve action plan.
 | No | Yes |
| 1. Implement action plan and provide on-going status until completion.
 | Yes | No |
| 1. Initiate the <AGENCY> plan in the event of a <AGENCY> situation per the <AGENCY> policies and procedures.
 | No | Yes |
| 1. Initiate the <AGENCY> plan in the event of a Contractor <AGENCY> situation and notify <AGENCY> per DR policies and procedures.
 | Yes | No |
| 1. Coordinate with <AGENCY> during a Contractor <AGENCY> situation per <AGENCY> policies and procedures.
 | Yes | No |

#### Disaster Recovery Services

The Contractor must demonstrate that it will consistently meet or exceed <AGENCY> IT Disaster Recovery Plan requirements, and shall comply with any federal requirements on Continuity and DR. The following table identifies Disaster Recovery Services roles and responsibilities.

Table - Disaster Recovery Roles and Responsibilities

| **Data Management Roles and Responsibilities** | **Provider** | **<AGENCY>** |
| --- | --- | --- |
| 1. Recommend Disaster Recovery (DR) procedures that comply with Federal regulations (e.g., NIST 800-34, etc.)
 | Yes | No |
| 1. Develop, document, and maintain in the Standards and Procedures for DR and Continuation of Operations (COOP) procedures that meet <AGENCY> requirements and adhere to <AGENCY> policies.
 | Yes | No |
| 1. Review, provide additional procedures as required and approve DR and COOP procedures.
 | No | Yes |
| 1. Maintain ITRF and LRF through direct support or through 3rd party services (e.g., warranty and maintenance) as approved by <AGENCY>.
 | Yes | No |
| 1. Facilitate implementation of <AGENCY>’s IT Disaster Recovery Plan (DRP). The DRP includes requirements for IT Recovery Facilities (ITRF) to include: ITRF Hot Site, ITRF Cold Site, Work Area (LRF – Local Recovery Facility), Communications Services, Hosting Services, Backup/Data replication Services, and physical transport and storage of backup media. The Contractor shall provide and maintain the physical ITRF facilities, Hosting Services, and Backup/Data replication Services with redundant electrical, mechanical and network infrastructure; including, but not limited to HVAC, fire detection and suppression, electric power (primary and backup), UPS, Backup Generator, security system, and communications.
 | Yes | No |
| 1. Furnish all necessary facilities and equipment, supplies and materials, communications services, security, office and storage space, training, documentation, and other consulting/support services as required to perform the DRP service unless noted.
 | Yes | No |
| 1. Provide all technical and operations staff support, assistance, and services for all computing resources up to the operating system level before, during and after testing and in the event of a declared disaster for all provided IT equipment.
 | Yes | No |
| 1. Provide bi-annual DR testing time of two (2) forty-eight-hour sessions each for <AGENCY> to ensure that the <AGENCY>’s disaster recovery plans can be implemented successfully at the Contractor’s Recovery Facilities (current DR testing is conducted in February and August of each year).
 | Yes | No |
| 1. Acquire and manage consumables, such as tape, disks, etc., in support of the DRP requirements. Coordinate acquisition of additional materials as needed.
 | Yes | No |

The Contractor shall provide:

1. ITRF Hot Site, ITRF Cold Site, LRF

The Contractor shall provide one (1) or more fully operational ITRF Hot Sites that can be used to test the DRP and recover <AGENCY>’s IT operations for <AGENCY> MA and GSS systems. The Hot Site(s) will be provided within twenty-four (24) hours of a disaster declaration, or when <AGENCY> is ready to occupy a Hot Site. The Hot Site shall be provided for a period of up to six (6) weeks occupancy for each disaster declaration, and for additional six (6) week periods if requested, for a total of fifty-two (52) weeks occupancy, provided the facility is not otherwise occupied by other customers. After the <AGENCY>’s facility has been restored, the Contractor shall provide use of the Hot Site (and/or Cold Site and LRF) for a period of up to three (3) additional weeks of occupancy while the <AGENCY>’s IT operations is moved from the Contractor’s Hot Site (and/or Cold Site and LRF) site to the restored <AGENCY> facility. The three (3) week period is in addition to the initial six (6) week-period referenced above. An <AGENCY>’s designated representative will notify the Contractor at least one (1) week prior to the planned date to reoccupy the recovered <AGENCY> facility.

The ITRF Hot Site, Cold Site and LRF facilities and all their components shall be fully operational twenty-four (24) hours per day, 365 days per year (366 days in a leap year)

One ITRF, that satisfies the Recovery Requirements for Hot Site, shall be located between 20 and 70 miles from XXX. Additional ITRF Facilities must be located within the forty-eight (48) contiguous United States. (Overseas recovery facilities will not be accepted.) All facilities shall be located within fifty (50) miles of a national and/or interstate highway and national or international airport with regularly scheduled passenger service.

The Contractor shall also provide one (1) or more secondary ITRF (Cold Sites) for

<AGENCY>’s use in the event of an extended outage lasting longer than six (6) weeks. The Cold Sites may be co-located with the Hot Sites to minimize the transition from Hot Site to Cold Site services in the event of an extended disaster. Each of the above elements of the Recovery Facility, if not co-located in same building, will be linked with a high-speed wide area network (WAN) at 1 GB or higher.

The Cold Site will be populated with the customer’s IT requirements during the Hot Site occupancy period and will remain available to the customer for up to one year or more. The location and distance requirements for a Cold Site, which replaces a Hot Site, shall be the same as the Hot Site requirements listed above. <AGENCY> will be responsible for procurement of IT HW, equipment and software required to establish data center operations and communications at the cold site. The Contractor shall provide, at a minimum, one cold site that can accommodate <AGENCY>’s IT requirements.

In the event of a multiple disaster situation, wherein the Hot Sites or LRF provided under this contract are fully utilized by other subscribers, the Contractor may recover the <AGENCY>’s operations on systems and facilities provided by another disaster recovery vendor with equivalent capabilities with the <AGENCY>’s prior approval, and at no additional cost to the government.

The Contractor shall provide one or more LRFs (i.e., work areas). Each LRF shall be a fully outfitted end user office environment co-located with or connected by a high-speed WAN at 1GB or higher to the Hot Site (or Cold Site) facilities used to test <AGENCY> DR plan and recover <AGENCY>’s MA and GSS systems in the event of a declared disaster. The LRF shall be available within twenty-four (24) hours of disaster declaration, or when the <AGENCY> is ready to occupy the LRF. The location and distance requirements for an LRF shall be the same as the Hot Site requirements listed above. The occupancy of the LRF shall be made available for the same time periods as the Hot Site (or Cold Site) listed above for a total of up to fifty-two weeks occupancy per disaster declaration.

Each LRF shall contain fifty (50) or more operational workstations or desks. Each workstation/desk will contain a working Windows PC connected to an Ethernet LAN using Category 5E or higher cable. Each end-user workspace in the LRF must consist of, at a minimum, a 52” or larger cubicle desk area separated by acoustical type panels in front and on both sides, chair with adjustable features, desk surface, filing/storage with one or more locking drawers, one (1) pad of paper, pen, sharpened pencil, eraser, stapler, and bag of paper clips. Additional end-user requirements include the following:

* PBX/VOIP Phone with voice mail, Automated Call Distribution, and capabilities to support a central Call Center environment;
* Redundant connectivity to the common local carrier for Phone and Internet services
* Individual and/or common printer resources;
* Facsimile and copy capabilities
1. Communications Services – Internet Access

The Contractor will provide all Recovery Facilities with redundant and carrier diverse high- bandwidth Internet access, and VPN remote access technology.

In order to assure continuous availability of data communications resources for Recovery Facilities, the Contractor must provide at least two (2) geographically dispersed fiber feeds from separate Tier 1 backbone providers. Each carrier must provide its own electronics at the Contractor’s site so that the compete loss of one provider or fiber route will not result in the loss of Internet access.

At time of disaster and plan test, the Contractor shall make available for each Hot Site, Cold Site and LRF (for disaster declaration only) the following communications accesses.

* Two (2) 1GB or higher redundant Internet access lines

The <AGENCY> may obtain long-distance telecommunications circuits and/or services from the General Services Administration (GSA) Networx and WITS3 network providers between

<AGENCY> and the ITRF. The Contractor will be responsible for coordinating circuit installations at its Facilities, extending Point of Presence (POP) and Demarcation point for circuits into its Recovery Facility, and provide floor and rack space for Networx provider equipment. The Contractor will be responsible for provisioning any Border router and appropriate router interface cards to connect to network provider’s equipment and circuits

The Recovery Center must be equipped with a VPN concentrator to support secure outside data access during recovery operation.

1. Hosting Services

The Contractor shall provide Managed Hosting and Co-location services for pre-configured, <AGENCY>-dedicated recovery servers for MA and GSS Systems, at the request of <AGENCY>. The Contractor, as required by the COTR, will provide services to build and configure servers and related HW that are hosted and kept operational, within the Contractor’s secure hosting facility. <AGENCY> will maintain control of the government or Contractor provided servers. Full root or administrator access will be given to designated <AGENCY> system administrators.

The Contractor will provide secure remote access to the servers, including KVM over IP and include the capability to power on/off, reboot and load data from the <AGENCY> site in XXX to the hosted servers over a high-speed WAN at speeds between 100Mbps, that can be increased in 100Mbps increments to 1GB or higher. Assigned IP numbers must be provided for servers accessible via the Internet.

As directed by the COTR, the Contractor shall provide the following services:

* + Pre-defined, alternate DNS routing for web-based application recovery
	+ Server administration
	+ Upgrades of OS and Security patches, hot-fixes, OS upgrades and service packs
	+ Repair and routine maintenance of hardware
	+ Monitoring and troubleshooting of the servers 24/7
	+ Tools to monitor web site and application performance
	+ Bandwidth utilization reports
1. Media and Electronic Backup Support Services

The Contractor shall maintain an offsite storage facility to store electronic data and hardcopy back-up records. The Contractor will perform all offsite tape storage activities including: pick up and return of electronic data media materials; pick up of paper back-up documents; ad hoc and unscheduled pick-up and return of electronic data media or paper documents when requested; long-term storage of electronic data media; and delivery of electronic data media to Hot and Cold sites during DR testing and declared disaster. Tapes must be cataloged, and inventory tracked by individual tape using the bar codes on the tapes. The Contractor will provide monthly storage and activity reports.

The Contractor shall also provide on request services for electronic off-site storage and retrieval of <AGENCY>’s backup data, including electronic transmission of data over dedicated communication circuits to the Contractor’s Recovery Facilities with capability to support Virtual Tape Libraries (VTL), disk based backup, remote database journaling and log shipping; r-sync of files and directories, and disk storage replication. The Contractor shall also support 3rd party Cloud based Backup services on request to the ITRF Hot and Cold sites.

1. Disaster Declaration Procedures

The Contractor must provide a detailed description of its disaster declaration procedures, including but not limited to process to identify the names and phone numbers of the

<AGENCY> personnel authorized to declare a disaster; authorization code and/or password to be used when declaring a disaster; Contractor policies and procedures for declaring alerts and disaster events; and methods for resolving problems.

For purposes of this SOW, the following definitions apply:

Hot Site: A fully operational configured computing facility/data center that requires only installation of system and application software and establishment of communication arrangements to any government facility and/or network to implement the <AGENCY>’s DRP.

<AGENCY> will provide its own software, which includes application software, database, and other systems software. The Hot Site is provisioned with redundant electrical, mechanical and network infrastructure containing shared, vendor provided information technology equipment, such as UNIX/Windows servers, SANs, tape and disk backup systems, remote access, and other appliance HW, switches, routers, firewalls, personal computers, and printers. Customers can make immediate use of Hot Site technology assets to recover from a disaster and can also periodically test their DR plan by simulating disaster events. In the event of an actual disaster, customers will occupy the Hot Site and utilize facility/data center to reconstitute their operations for a fixed period of time.

Cold Site: Data center facilities/data center with redundant electrical, mechanical and network infrastructure that can be used by Hot Site customers for an extended period of time after their Hot Site occupancy period has expired. The Cold Site will be populated with the customer’s HW requirements during the Hot Site occupancy period and will remain available to the customer for up to one year or more.

Work Area – Local Area Network/Workstation Recovery Facilities (LRF): A fully outfitted end user office environment co-located with or connected at high speed to Hot Site facilities which is accessed on a shared-risk basis and available for the same duration as the Hot Site.

Workspaces are equipped with a Windows PC or virtual desktop, PBX/VOIP phone with Automated Call Distribution (ACD)/Voice mail, desk and chair and have access to meeting and conference facilities and amenities such as secure parking, kitchens, sleeping quarters and lounge areas.

Hosting: Secure data center facilities used to provide Managed Hosting and Co-location services used to support the mission critical applications which are provisioned with redundant, concurrently maintainable electrical, mechanical and network infrastructure. The equipment may be vendor managed or customers may locate their own equipment for production or disaster recovery purposes. Hosting facilities provide direct connectivity to all major Tier 1 network providers, scalable power and cooling resources and on-site support services.

## Projects

The Contractor shall perform studies, analyses and provide other technical services in support of DIS objectives. Such studies/analyses may include, but are not limited to logistics/supportability, engineering, financial, operational, and business processes. The Contractor shall perform non-recurring engineering studies and analyses to evaluate the viability of potential solutions, alternatives to various technical issues and challenges, and emerging products or technology. The Contractor shall perform the evaluation of unproven technology applications and identification of potential risks. The development of pre-production or COTS- based prototypes may be required.

As required the Contractor shall furnish schedules and budgets (T&M and FFP – as required) for various project work as defined by <AGENCY>.

## Surge Labor

The Contractor will provide additional services for additional capacity as required by the Government. The Government estimates that this “surge” demand will not be greater than 20 percent of Operations and Maintenance and/or Contract, Program and Project Management sections detailed above.

## Other Direct Costs / Travel

The Government will reimburse the Contractor on the basis of actual cost plus the Contractor’s approved Materials Handling fee for items approved by the COTR.

## Hardware / Tools

The Government will reimburse the Contractor on the basis of actual cost plus the Contractor’s approved Materials Handling fee for items approved by the COTR.

## Contract Access Fee

The Government will reimburse the Contractor on the basis of actual cost of the Contract Access Fee (CAF) on an annual basis. The Contractor shall pay the Contract Access Fee to the Agency designated, and within the terms contained with the Contract Vehicle.

# Service Management

## Objectives

The following objectives are key to achieving customer satisfaction. At a high-level service management support objectives <AGENCY> expects, and that the Contractor shall endeavor to meet:

* + - Reduce Service Delivery Time and Cost – Improve the productivity of <AGENCY> transactions and process through training and process improvement. Improve the operations, while reducing the administrative burden by streamlining compliance processes;
			* Rapid adjustment in changes to established standards, processes, and tools
			* Continuous improvement in results as measured against Service Level Objectives and other performance standards
		- Ensure that critical IT life cycle and service management functions are included in the response to this SOW and any and all future service requests.
			* Provide pro-active concepts and forward-looking leadership in service delivery
			* Maintain cost effective services that are on par with industry practices
		- Manage services with systemic with enterprise views across all IT service areas such that proactive communication with other Contractors and/or functional groups of

<AGENCY> are consulted/considered in planning or addressing all management and financial matters.

* + - Maintain alignment with business needs by thoroughly planning, and executing activities in an effective, flexible, and responsive manner
		- Facilitate and ensure continuous, cross-team coordination (e.g., <AGENCY> and other Contractors) of all technical activities within the functional areas described in this SOW.
			* Timely response and support of new initiatives and requests
			* Accuracy of information

As such, the Contractor shall be responsible for providing Support Services defined throughout this SOW and as detailed in the sections below.

## Project Key Performance Parameters

Key Performance Parameters (KPPs) represent those capabilities or characteristics so significant that failure to meet them can be cause for the concept or selected system to be reevaluated, or the program to be reassessed or terminated. The threshold value is the minimum acceptable value that, in the <AGENCY>’s judgment, is required to satisfy the need. If threshold values are not achieved, program performance is seriously degraded, the program may be too costly, or the program may no longer be timely. The objective value is that desired by the user and which the program manager is attempting to obtain. The objective value could represent an operationally meaningful, time-critical, and cost-effective increment above the threshold for each program parameter.

<AGENCY> will measure Service delivery against key performance parameters and Service Level Requirements (SLR), which shall be developed during the Transition Period by the Contractor and approved by <AGENCY>.

Measuring customer satisfaction across the lifecycle of any project is important for measuring the quality of delivery. The intervals at which customer satisfaction should be measured will be early and often (i.e., quarterly) at the beginning of the contract in order to baseline customer expectations for the application and or system. As the contract progresses measurement intervals may decrease to semi-annually or annually using the measures captured in the onset of the project in order to map progress for increasing system quality and effectiveness. The COTR will be the conduit through which customer satisfaction shall be measured. The COTR is responsible for canvassing Senior Executives from technical and business/mission/customer organizations and Project Leadership, Managers and Operators from the Government for feedback.

The areas for customer satisfaction survey denoted below shall be included as a part of the customer survey. These measures will be revisited annually to determine if they still best meet the Government’s needs.

### Customer Satisfaction Metric

#### Purpose

The purpose of this section is to provide <AGENCY> a specific Service Level Agreement (SLA) that serves as the key measure of the Contractor’s performance.

#### Service Level Agreements

IT Infrastructure Support Services are defined in Part II of this SOW as the operations and maintenance of the data center, server infrastructure, network – including telephony – infrastructure, database systems, identity management, desktop management, tier 2 and 3 helpdesk and access to SMEs. <AGENCY> will concentrate management in two (2) areas, the first area – **COTR’s Assessment**. COTR Assessment is a monetary metric that captures the subjective opinion of the major Stakeholders / Customers through the COTR Assessment to ensure that requirements are being met and delivered.

The second area – **Operational Metrics** – relies upon metrics that demonstrate technical and business performance of the services contracted by the Government.

#### Corrective Action Plan

In the event that any Operational Measures are consistently missed, as determined by the COTR, the Government can request that the Contractor develop a “corrective action plan” that details the nature of the problem, what actions are required to remedy the situation, any potential risks and risk mitigation strategies.

#### Measurement Period

For the first six (6) months of the Base Period, the Contractor shall measure, and report results of both Monetary and Operational metrics; however, performance will not be positively or negatively incentivized. After the six (6) month acclimation period has expired, monetary incentives will be appropriately incentivized, per each measure’s description.

#### Monetary Metric

A single monetary metric is associated with the performance of this scope of work.

#### COTR’s Assessment

Measuring customer satisfaction across the lifecycle of any project is important for measuring the quality of delivery. The intervals at which customer satisfaction should be measured will be early and often (i.e., quarterly) at the beginning of the contract in order to baseline customer expectations for the application and or system. As the contract progresses, measurement intervals may decrease to semi-annually or annually using the measures captured in the onset of the project in order to map progress for increasing system quality and effectiveness. The COTR will be the conduit through which customer satisfaction shall be measured. The COTR is responsible for canvassing Senior Executives from technical and business/mission/customer organizations and Project Leadership, Managers and Operators from the Government for feedback.

The areas for customer satisfaction survey denoted below shall be included as a part of the customer survey. These measures will be revisited annually to determine if they still best meet the Government’s needs.

All elements will utilize a 0-4 scale score, with a final 0-4 Overall Score assigned.

* + - * **Reliability** – Time and attendance or personnel, responsiveness to requests, attention to system stability
			* **Deliverable Quality** – Compliance with <AGENCY> processes and procedures, quality and timeliness of deliverables and reports,
			* **Mission Effectiveness** – A measurement of the level to which personnel participate and offer solutions and recommendations that support operational and business requirements,
			* **Project Communication / Documentation** – A measurement of usefulness, clarity, completeness, and correctness of project communications and documentation including, but not limited to, any documentation required by <AGENCY>.
			* **Open Comments** – A data collection method to gather insight and input from the surveyed community. Information gathered is used to provide context to the other survey. Open Comments shall be included at the end of each measurement section soliciting input for areas of improvement, success, and other comments.
			* **Overall Project Satisfaction** – A synthesis of all elements of the survey resulting in a single rating for the Contractor’s performance during the assessment period. The PM will use the areas designated as well as draw upon additional experience with the Contractor outside or beyond the measures provided in the survey to arrive at a final assessment. In the case of multiple PMs, a single consensus Overall Project Satisfaction score will be provided.

Scale Definitions:

* + - **0 Unsatisfactory** – Service expectations did not meet the PM(s)’s expectations. Numerous examples of the Contractor’s poor performance are documented through deliverables, meeting minutes, emails, etc. Corrective actions are contemplated or have already been discussed with the Contractor.
* **1 Less than Satisfactory** – Service failed to meet expectations in one or two critical areas.
* **2 Satisfactory** – Service met expectations and represents a good value to the Government for the resources expended.
* **3 More than Satisfactory** – Service exceeded the services expectations proposed in the technical proposal and provided real benefit to <AGENCY>.
* **4 Exemplary** – Service far exceeds what was proposed and provides significant positive impact to <AGENCY>. Examples of the Contractor exceeding the level of service contracted for are documented through deliverables, meeting minutes, emails, etc.

Table – Service Level Agreement #1

| **Item** | **Description** |
| --- | --- |
| **SLA Over View** |  Blank Cell |
| 1. Task Area:
 | IT Infrastructure Support Services |
| 1. Performance Category:
 | Quality |
| 1. SLA #:
 | 1 |
| 1. SLA Name:
 | COTR’s Assessment |
| **SLA Overview** | Blank cell |
| 1. SLA Description:
 | <AGENCY> satisfaction with Contractor delivery management of IT Infrastructure Support Services, as assessed by the COTR. |
| 1. Performance Period:
 | This SLA is in effect on a continuous basis without interruption throughout the Period of Performance. |
| **SLA Metrics** | Blank cell |
| 1. Measurement Interval:
 | The Measurement Interval is three (3) months for first year and then every six (6) months thereafter. |
| 1. Measurement Period:
 | The Measurement Period begins at 00:01 on the first day of the month and ends at 24:00 on the last day of the month. |
| 1. Source of Measurement Data:
 | Data will be collected from management surveys containing satisfaction criteria specified by <AGENCY> that is either developed internally by<AGENCY> personnel or by <AGENCY>-selected impartial 3rd party. |
| 1. Method of Surveillance:
 | Performance will be measured via Customer Feedback. <AGENCY> will issue customer satisfaction surveys to designated PM. The scale is: a zero to four-point scale (0) Dissatisfied, (1) Less than Satisfied, (2) Satisfied, (3) More than Satisfied, (4) Exemplary. |
| 1. Timing of Measurement:
 | Measurements are taken within five (5) days of the end of the Measurement Period. |
| 1. Exceptions:
 | Field left blank intentionally. |
| **SLA Measurement** | Blank cell |
| 1. Calculation:
 | The COTR’s overall assessment value |
| 1. Target Criteria:
 | A survey response of Satisfied, More Than Satisfied, or Exemplary |
| 1. Minimum Acceptable:
 | A survey response of Satisfied, More Than Satisfied, or Exemplary |
| 1. Definitions:
 | None. |
| **Incentive** **Administration** | Blank cell |
| 1. Incentive Type:
 | Negative Incentive of “at risk pool” for Overall Survey results of Dissatisfied and Less than Satisfied. No incentive for Satisfied or More than Satisfied. A positive incentive of X for a survey result of Very Satisfied. |
| 1. Incentive Calculation:
 | TBD - [vendor to propose the incentive value] |
| **SLA Administration** | Blank cell |
| 1. Reporting Frequency:
 | Reporting to commence upon Contract Award and continue throughout the Period of Performance.Quarterly survey reporting from <AGENCY> PM during first year, semi-annual thereafter. |
| 1. Notes and Comments:
 | None. |

Note: Although Customer Satisfaction service level agreement is a measure of the overall performance of the Contractor; it is heavily affected by issues with or successes by individuals (Contractor resources) and their participation and value to the activities and areas for which they are responsible.

The KPPs in Attachment A – Service Level Requirements represent the current set of operational measures applied to services at <AGENCY> for which <AGENCY> expects to be consistently met or exceeded. From time-to-time these SLRs can change or reclassified to reflect changing levels of “Business Criticality” and the potential “Business Impact and may be re-classified as needed by the Government comply with regulatory requirements (e.g., Federal Regulations, OMB circulars, and other regulations).

The Contractor shall provide written reports to <AGENCY> regarding Contractor’s compliance with the SLR specified in this SOW (Attachment A).

Table - Service Level Monitoring Roles and Responsibilities

| **Service Level Monitoring Roles and Responsibilities** | **Provider** | **<AGENCY>** |
| --- | --- | --- |
| 1. Approve and document SLR and reporting cycles.
 | No | Yes |
| 1. Document SLR requirements and agreements.
 | Yes | No |
| 1. Report on service performance improvement results.
 | Yes | No |
| 1. Coordinate SLR monitoring and reporting with designated <AGENCY> representative(s) and third-party vendors, as required.
 | Yes | No |
| 1. Measure, analyze, and provide management reports on performance relative to requirements.
 | Yes | No |
| 1. Develop SLR improvement plans where appropriate.
 | Yes | No |
| 1. Review and approve improvement plans.
 | No | Yes |
| 1. Implement improvement plans.
 | Yes | No |
| 1. Review and approve SLR metrics and performance reports.
 | No | Yes |
| 1. Provide <AGENCY> with portal access to performance and SLR reporting and monitoring system.
 | Yes | No |
| 1. Follow existing mechanisms for continuous improvements and equitable service management (e.g., Balance Scorecard, Value Engineering, Engineering Change Process, Service Request Reviews), and recommend changes as appropriate.
 | Yes | No |

# Referenced SOW Appendices and SOW Schedules

Table – Referenced SOW Appendices and SOW Schedules

| **SOW Appendix** | **Description** |
| --- | --- |
| 1. C0 Current State
 | [See SOW] Brief Description of the overarching Product and Service Objectives |
| 1. C1 End User Hardware
 | Asset information for active and idle devices that will fall under Desktop Management, e.g., desktops, laptops, workstations, handheld devices. |
| 1. C2 End User Core Image Software
 | Core Image by Mode / Department Function and list of software comprising image |
| 1. C3 End User Non- Core COTS Software
 | All shrink-wrap / Commercial-off-the-Shelf (COTS) software in use but not part of core image |
| 1. C4 End User Non- Core GOTS Software
 | All Government-off-the-Shelf (GOTS) software in use but not part of core image |
| 1. C5 <AGENCY>
2. Locations
 | Place of Performance and Primary Points of Contact |
| 1. C6 Current Agreements/Contracts
 | Agreements and Contracts that potentially impact scope (e.g., warranty considerations), involve similar projects (upgrading systems), or potentially create conflict (e.g., break/fix, IMACs). |
| 1. C7 Current, In Progress Projects
 | Example: SharePoint, Virtualization |
| 1. C8 Future Projects and Initiatives
 | Example: Network Upgrades, Planned Refresh |
| 1. C9 Historical Email Ticket Volume
 | Previous eight (8) Quarters |
| 1. C10 Servers
 | Server Configurations (include Direct Attached Storage) |
| 1. C11 Storage
 | SAN & Tape |
| 1. C12 Backups
 | Backup Policies, Customer Agreements, and Service Level Agreements |
| 1. C13 Network
 | Asset information for active and idle devices that will fall under the Network Infrastructure, e.g., routers, switches, appliances. |
| 1. C14 Enterprise Architecture
 | Network Topology, Cubes, Patterns, Bricks, etc. |
| 1. C15 Enterprise Applications
 | Current Enterprise Applications (i.e., FastLane, eJacket, R.gov, etc.) |