Information Technology A-76 Study

U.S. Department of Energy

PERFORMANCE WORK STATEMENT

Submitted to:

Laura Rodin, PWS Team Leader
U.S. Department of Energy
1000 Independence Avenue, SW
Washington, DC 20585

November 3, 2003

TABLE OF CONTENTS

TECHNICAL EXHIBITS (TE):

SECTION 1: INTRODUCTION

1.1 Overview

This document is a Performance Work Statement (PWS) for a performance-based support services contract. The purpose of this PWS is to describe the performance objectives for Information Technology (IT) services for the Department of Energy (DOE) at multiple DOE sites nationwide. For purposes of this document, the term "Service Provider (SP)" refers to either the Government or private sector organization that will serve as an integrator to develop, assemble and execute a comprehensive solution to complex IT requirements. This document contains information available at the time of publication relating to administrative and technical responsibilities, performance requirements, and workload estimates for DOE IT services. The SP shall exercise management and operational control over and retain full responsibility for performance requirements set forth in this PWS. Offerors are encouraged to incorporate process improvements and industry best practices in their proposals. The SP may introduce new technologies and processes in partnership with customers, in order to deliver the best value products or services. The scope of this A-76 study includes the workload and efforts of both Federal employees and support contractors currently performing the respective requirements across multiple locations.

1.2 Background

The President's Management Agenda (PMA), issued in the summer of 2001, establishes an aggressive strategy for improving the management practices of the Federal Government. The Agenda focuses on five initiatives that present a substantial opportunity for improvement across the Federal Government. One of these initiatives is to establish and sustain Competitive Sourcing Initiatives for Defense and Civilian Agencies.

The Competitive Sourcing Initiative requires Federal Agencies to subject commercial activities (CA) performed by Federal employees to competition with the private sector. This process determines whether it is more efficient and cost effective to have the commercial activities performed by Federal employees or by a contractor. In order to comply with Office of Management and Budget (OMB) Circular A-76, DOE must compete a portion of its commercial activities from the Federal Activities Inventory Reform (FAIR) Act inventory. As a result, DOE is conducting a Competitive Sourcing Study of the IT function across the agency.

1.2.1 History

The Government has long been involved in the energy needs of the nation from the establishment of alternating current as the standard for electricity production, transmission, and use in the U.S., through a century of vast energy (and often labor) related projects including the Hoover Dam, the Tennessee Valley Authority, and others. The nuclear and defense origins of the DOE can be traced to the Manhattan Project and the development of the atomic bomb during World War II. In 1942, the U.S. Army Corps of Engineers established the Manhattan Engineer District, which later became the Atomic Energy Commission.

The extended energy crisis of the 1970s pointed out to the nation the ineffectiveness of the many energy and nuclear related Government agencies in dealing with their problems systematically. Public demand prompted the decision to unify the nation's planning, research, and policy development into a single organization to deal with energy, including all aspects of the energy released from the nucleus of atoms. The resulting DOE Organization Act brought the Federal Government's agencies and programs into a single agency and abolished the Atomic Energy Commission. On October 1, 1977, DOE assumed the responsibilities of the Federal Energy Administration, the Energy Research and Development Administration, the Federal Power Commission, and parts and programs of several other agencies.

Nationwide, DOE employs approximately 14,500 Federal and 100,000 contractor employees in a complex that consists of Headquarters (HQ) and field organizations, national laboratories, nuclear weapons production plants, power marketing administrations, and special-purpose offices at over 50 major installations in 35 states.

For more information on DOE, see the DOE Website @ http:\\www.energy.gov.

1.2.2 DOE Mission Statement

DOE's overarching mission is to advance the national, economic, and energy security of the United States; to promote scientific and technological innovation in support of that mission; and to ensure the environmental cleanup of the national nuclear weapons complex. The Department has four strategic goals aimed at achieving the mission.

- **Defense:** To protect our national security by applying advanced science and nuclear technology to the Nation's defense.
- **Energy:** To protect our national and economic security by promoting a diverse supply of reliable, affordable, and environmentally sound energy.
- **Science:** To protect our national and economic security by providing world-class scientific research capacity and advancing scientific knowledge.
- **Environment:** To protect the environment by providing a responsible resolution to the environmental legacy of the Cold War and by providing for the permanent disposal of the Nation's high-level radioactive waste.

1.2.3 Office of Chief Information Officer Mission Statement

The Office of the Chief Information Officer (OCIO):

- Provides advice and assistance to the Secretary of Energy and other senior managers to ensure that information technology is acquired and information resources are managed in a manner that implements the policies and procedures of legislation, including the Paperwork Reduction Act and the Clinger-Cohen Act; and the priorities established by the Secretary.
- Coordinates and articulates a shared vision and corporate perspective among the Department's information activities and champions Departmental initiatives to effectively manage information and to provide for corporate systems that add value to the businesses of the Department.
- Ensures that information created and collected by the Department is provided to appropriate internal and external customers and stakeholders in a timely, cost-effective and efficient manner.

1.3 Document Layout

The following indicates the structure of the PWS.

1.3.1 PWS Structure

This PWS is structured according to sections and relevant Technical Exhibits (TE) as follows:

1. Introduction
2. Scope of Work
   - TE 2-1: Users by Program/Staff Office
   - TE 2-2: Users by Physical Location
3. Performance Objectives and Measures
   - TE 3-1: Historical Workload Estimates
   - TE 3-2: Performance Requirements Summary
   - TE 3-3: Required Reports
   - TE 3-4: IT Infrastructure
   - TE 3-5: Existing Maintenance Agreements and Warranties
   - TE 3-6: SP Supported Equipment
   - TE 3-7: SP Supported Software and Applications
4. Key Personnel
5. General Requirements
   - TE 5-1: Security Clearance Requirements

6. Government Furnished Property and Services
    - TE 6-1: Government Furnished Facilities
    - TE 6-2: Government Furnished Equipment
    - TE 6-3: Government Furnished Software and Applications
7. Service Provider Furnished Property and Services
8. Continuity of Operations
9. Quality Control and Quality Assurance

Appendix A: Definitions and Acronyms
Appendix B: Technical Library (Regulations/Directives)

1.3.2 Technical Exhibits

Technical Exhibits are used to provide supplementary information and can be in the form of tables, graphs, maps, etc. TEs provided in this PWS may be referenced from any section, and are identified by the letters "TE" followed by a space, the related Section number, a dash, and sequence number of the individual TE from that section (e.g., TE 3-1). To avoid confusion in this document, TEs are referenced by italics, followed by a colon, two spaces, and the name of the TE (e.g., *TE 3-3: Required Reports*).

SECTION 2: SCOPE OF WORK

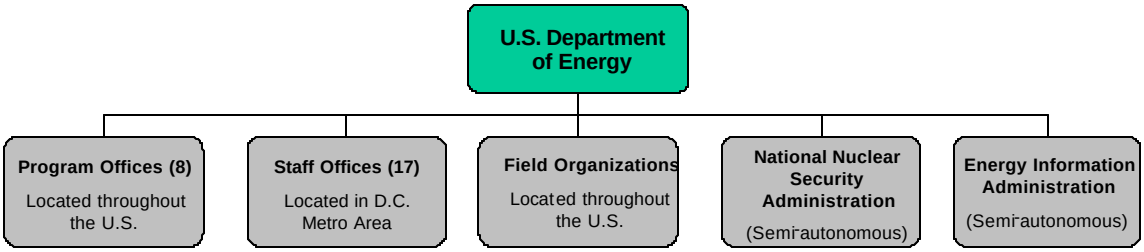
2.1 Work Description

Information Technology is defined as computing, telecommunications, and information services. The SP shall be the support DOE's objectives in the following four major functional areas, which are detailed in Section 3:

- **Information Technology Management** – Activities related to management support of IT related policy development, strategic planning, capital planning, resource management, and special projects.
- **Systems Development and Engineering** – Activities pertaining to software development support for all existing, planned, and future DOE IT systems. Typical duties include capturing user and business owner requirements; coordinating with appropriate Departmental personnel regarding enterprise architecture; identifying functional, security and performance requirements; developing logical and physical database models; performing coding, testing, quality assurance, design and program documentation; implementation; and maintaining interoperability between future and existing hardware and software applications. Software applications include, but are not limited to, web applications, Commercial-Off-The-Shelf (COTS) integration, Government-Off-The-Shelf (GOTS) integration, and custom applications development.
- **Operations Support** - Activities related to planning and implementing telecommunications and information technology infrastructures; network administration which may include network access and security; server management; IT disaster recovery planning and execution; IT inventory control; audio, video, and web conferencing; user support; training and education; wireless services; spectrum management; voice and data services; web services; and IT related surveillance systems.
- **Cyber Security** - Activities related to the secure transmission and storage of electronic information, drafting policy, procedures, user awareness training, planning, budgeting, risk management, internal and/or external auditing. Further cyber security activities pertain to selecting and supporting the use of electronic security hardware and software tools and mechanisms including, but not limited to, encryption devices, access control, user identification and authentication, and malicious content detection.

2.2 Organizational Landscape

DOE carries out its mission through eight (8) Program Offices and two (2) semi-autonomous Program Offices. Seventeen (17) Staff Offices provide support to the Program Offices. The following diagram provides a high-level depiction of DOE's structure.



2.2.1 Program Offices

A Program Office is responsible for executing program management functions, and for assisting and supporting Field Offices in safety and health, administrative, management, and technical areas. The Program Offices also identify, develop, and direct various policies and programs to accomplish the Department's mission. The eight (8) major Program Offices are as follows:

- Civilian Radioactive Waste Management (RW)

- Energy Efficiency and Renewable Energy (EE)
- Environment, Safety and Health (EH)
- Environmental Management (EM)
- Fossil Energy (FE)
- Nuclear Energy, Science, and Technology (NE)
- Science (SC)
- Worker and Community Transition (WT)

For individual missions and more information on these program offices, see *TE 2-1: Users by Program/Staff Office*. Most Program Offices maintain workforces in both Washington, DC metro area headquarters offices as well as in field organizations throughout the United States. Some Program Offices have staff in several different field organizations, whereas others maintain staff in only one location.

2.2.2 Staff Offices

The sixteen (17) Staff Offices of DOE are administrative in nature and support the mission-related Program Offices. All staff offices are headquartered in the Washington, DC metropolitan area; however some staff office employees are located in field organizations throughout the United States.

- Chief Information Officer (OCIO)
- Congressional & Intergovernmental Affairs
- Counter Intelligence (CN)
- Departmental Representative to the DNFSB
- Economic Impact and Diversity (ED)
- Energy Assurance (EA)
- General Counsel (GC)
- Hearings and Appeals (HG)
- Independent Oversight & Performance Assurance (OA)
- Inspector General (IG)
- Intelligence Office (IN)
- Management, Budget, and Evaluation (ME)
- Office of the Secretary
- Policy & International Affairs (PI)
- Public Affairs
- Secretary of Energy Advisory Board
- Security (SO)

2.2.3 Field Organizations

Field Organizations are located throughout the United States. Most field offices support Program Offices; however, some field offices provide support to multiple program offices. Field Organizations take several forms including Operations Offices, Field Sites, and Laboratories.

2.2.4 National Nuclear Security Administration

The National Nuclear Security Administration (NNSA) is a semi-autonomous program of DOE that focuses on administering policy in the area where energy and defense programs intersect. The mission of the National Nuclear Security Administration is:

- To enhance United States national security through the military application of nuclear energy.
- To maintain and enhance the safety, reliability, and performance of the United States nuclear weapons stockpile, including the ability to design, produce, and test, in order to meet national security requirements.
- To provide the United States Navy with safe, militarily effective nuclear propulsion plants and to ensure the safe and reliable operation of those plants.

- To promote international nuclear safety and nonproliferation.
- To reduce global danger from weapons of mass destruction.
- To support the United States leadership in Science and Technology

2.2.5 Energy Information Administration

The Energy Information Administration (EIA) is a semi-autonomous program of DOE that provides high quality, policy-independent energy information to meet the requirements of Government, industry, and the public in a manner that promotes sound policymaking, efficient markets, and public understanding. EIAs sole purpose is to provide reliable and unbiased energy information.

2.3 Customers

The scope of IT support provided under this PWS will be limited to Federal employees and the support contractors who occupy Federal space and require the same IT support as the Federal employees. The SP shall provide IT services with a customer-oriented approach. More information on the users across DOE is included in *TE 2-1: Users by Program/Staff Office and TE 2-2: Users by Physical Location*.

2.4 Work Locations

Workload to be performed by the SP under this contract is required at both Headquarters Offices in the Washington, DC metro area and in Field Organizations throughout the United States. More information on each location is included in *TE 2-2: Users by Physical Location*.

2.5 Enterprise Architecture

The Department is developing an Information Enterprise Architecture (EA) Program using the Federal Enterprise Architecture (FEA) reference models to standardize and improve IT management processes across the Department and the Federal Government. The Program has defined the foundations, baseline, guidance, standards, and vision for the development and implementation of an architecture-based process for making IT investment decisions. A primary tenet of the DOE information architecture methodology is that business needs drive the need for applications and technology, not vice versa. The architecture is used to assess legacy and development systems for alignment with key business, technical, and operational criteria. The SP shall support the development of the Department's EA.

The DOE Information Enterprise Architecture Program:

- Implements a Department-wide EA to support the acquisition and maintenance of information technology investments per the requirements of OMB Circular A-130, Information Technology Management Reform Act of 1996 (ITMRA a.k.a. Clinger-Cohen Act) and other guidance.
- Makes common, reliable data available for sharing Department-wide and minimizes redundant and duplicative systems.
- Completes, refines, and executes the Corporate Systems Information Enterprise Architecture.
- Provides leadership, education, and support to EA efforts.

2.6 Quality

Over the past decade, the Federal Government has mandated higher standards of quality through a series of initiatives (e.g. Government Performance and Results Act (GPRA), Clinger-Cohen Act, etc). To that end, the Government expects the SP to propose and implement an IT organization that supports the highest level of quality. The SP shall establish a quality element within its organization that ensures compliance with applicable Federal mandates, contractual performance standards, and industry best practices. The SP shall consider as part of its Quality Control Plan (QCP) a number of standard approaches toward quality such as the International Standards Organization (ISO) and Systems Engineering Institute/Capability Maturity Model (SEI/CMM) processes. For additional stipulations on quality, refer to *Section 9: Quality Assurance and Quality Control*. Specific quality requirements may also be provided at the individual task level.

2.7 Documentation

The SP shall be responsible for the documentation of all efforts to include, but not limited to contract provisions, network schematics, and any documentation associated with *Section 3: Performance Objectives and Measures*. Requirements associated with documentation may be task driven. For more information on the applicable laws and regulations relevant to documentation, see *Section 5.3: Reporting & Records Maintenance* and *Appendix B.1 Applicable DOE Directives and Orders and B.2: Other Applicable Directives and Orders*. See http:/cio.doe.gov/RBManagement/Records/records.html.

2.8 Configuration Management and Change Control

Configuration Management is the discipline of identifying all components and their relationships in a continually evolving system, taking into account relevant system interfaces, for the purpose of maintaining integrity, traceability, and control over change throughout the life cycle. It is a disciplined process of technical and administrative direction for the identification and documentation of a system's functional and physical design requirements; the management of subsequent changes; and the verification of successful requirement implementation.

DOE is continuously trying to align with evolving IT industry "best practices", the changing application of IT in the workplace, and Federal mandates. The SP shall assist DOE in the improvement of the Configuration Management processes. The discipline of Configuration Management applies to multiple tasks identified in *Section 3: Performance Objectives and Measures*. The SP shall be responsible for adhering to DOE Configuration Management standards in the performance of this Contract.

2.9 Program/Project Management

The DOE requires high quality, systematic program/project management as a factor in the accomplishment of planned project objectives and the realization of projected benefits. Project management has two tightly linked components: a business and a technical component. The business component focuses on project initiation and justification, project planning and control, and project evaluation and closeout. The technical component deals with requirements definition; technical design; acquisition or development; and testing, installation, and operation of hardware and software assets.

The SP shall be responsible for the day to day management of the project and delivering the means, methods, and resources to meet the contract end point requirements and the intermediate requirements that the Contracting Officer's Representative (COR) determined are value added and necessary to achieve project success. The SP shall ensure a seamless operating environment at all components of DOE throughout the lifecycle of this contract, including transition activities if and when the SP plans to introduce new technologies and functions.

The SP shall adhere to DOE Order (O) 413.3, Program and Project Management for the Acquisition of Capital Assets and DOE Manual 413.3-1, the framework and context for implementing DOE Publication (P) 413.1, Program and Project Management for the Planning, Programming, Budgeting, and Acquisition of Capital Assets. The SP shall also adhere to Office of Management and Budget 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.

2.10 Certification and Accreditation

Percentages of Federal IT systems in critical infrastructure areas have not completed needed security certifications, thus placing sensitive Government information and programs at risk and potentially impacting national and economic security. Security certifications provide agency officials with the necessary information to authorize the secure operation of those IT systems.

The SP shall comply with DOE Order 205.1 and National Institute of Standards and Technology (NIST) 800-37 *Guidelines for the Security Certification and Accreditation of Federal Information Technology*

Systems. NIST has developed the following principles to aid in developing a certification and accreditation strategy:

- Develop standard guidelines and procedures for certifying and accrediting Federal IT systems including the critical infrastructure of the United States;
- Define essential minimum security controls for Federal IT systems; and
- Promote the development of public and private sector assessment organizations and certification of individuals capable of providing cost effective, high quality, security certifications based on standard guidelines and procedures.
- The specific benefits of the security certification and accreditation (C&A) initiative include:
- More consistent, comparable, and repeatable certifications of IT systems;
- More complete, reliable, information for authorizing officials—leading to better understanding of complex IT systems and associated risks and vulnerabilities—and therefore, more informed decisions by management officials;
- Greater availability of competent security evaluation and assessment services; and
- More secure IT systems within the Federal Government.

2.11 Knowledge Management

DOE's intellectual capital - the knowledge that people gain through experience - if made accessible to DOE personnel, will minimize "reinventing the wheel" and ultimately reduce costs to the taxpayer. Therefore it is the intention of the Government to use Knowledge Management (KM) to develop and improve mission control, efficiency, and effectiveness.

The SP shall be responsible for providing and maintaining KM information associated with the execution of all performance requirements under this PWS. This information shall reside in DOE's corporate data repository. The SP shall consider any intellectual, structural, or customer capital, that is understood, contained, or generated in the execution of any task assignment as KM information. The information shared by the individuals responsible for such execution shall become the intellectual property of DOE. After reviewing the requirements of this PWS, the SP shall propose such a KM program.

SECTION 3: PERFORMANCE OBJECTIVES AND MEASURES

The SP shall provide an Enterprise Solution regarding Information Technology for DOE. The SP shall perform work at the direction of the COR in response to DOE issued performance requirements assignments. The main areas that are included in this PWS are IT Management, Systems Development and Engineering, IT Operations Support, and Cyber Security. The functions and activities include, but are not limited to the following:

- IT Management
  - Policy Development
  - Strategic Planning
  - Enterprise Architecture
  - Capital Planning & Investment Control
  - Resource Management
  - Procurement Actions
  - Special Projects
- Systems Development and Engineering
  - Application Development & Software Engineering
  - Web-Site Development/Maintenance
- Cyber Security
  - Cyber Resource Protection
  - Cyber Security Planning
  - Cyber Risk Management
- IT Operations Support
  - IT Facilities Management & Physical Security
  - Network Administration & Configuration
  - Firewall Management & Maintenance
  - Server Administration & Configuration
  - Application Systems Administration
  - Emergency Preparedness
  - Inventory Control
  - Maintenance, Support & Service Agreements Management
  - Audio, Video, and Web Conferencing
  - User Support
  - Workstation Management
  - Wireless Services
  - Voice & Data Services
  - Spectrum Management
  - Surveillance Systems

Note that each performance objective below has associated workload in *TE 3-1: Historical Workload Estimates*, and performance measures and standards referenced in *TE 3-2: Performance Requirements Summary (PRS)*. *TE 3-3: Required Reports* refers to reports required in each of the sections below, and includes the relevant reference number. *TE 5-1: Security Clearance Requirements* documents the security clearance levels required by each task.

3.1 Information Technology Management

The following subsections detail specific SP responsibilities pertaining to IT Management within the DOE organization including sensitive, classified and unclassified information systems. In support of IT Management activities, the SP shall comply with the Clinger-Cohen Act, the Paperwork Reduction Act, Government Paper Elimination Act (GPEA), Computer Security Act, Presidential Decision Directive (PDD) # 63, and the Government Performance and Results Act (GPRA) and other applicable laws and regulations. The SP shall provide expert consultation and perform work at the direction of the Designated Government Representative (DGR) in response to business needs.

IT Management tasks and sub-tasks are likely to include, but are not limited to, assisting with: developing, implementing, and monitoring Department-wide, program specific, and local IT policies, directives, orders, standards, Standard Operating Procedures (SOP), guidelines, and procedures; updating and submitting of Enterprise Architecture recommendations; Capital Planning and Investment Control; Resource Management; Budget Formulation and Execution; Department Strategic Plans, according to the guidelines and initiatives, as put forward by the Secretary of DOE. SP work under this contract shall also include products developed in response to quick-turnaround needs. Products shall include briefings, presentations, fact sheets, as well as issue and reference papers. The SP shall also assist in providing appropriate internal and external organizations information in the accomplishment of the overall IT mission. Coordination includes, but is not limited to, working with customers, other agencies, Congress, internal DOE program offices and field sites, and other external entities. When requested, the SP shall assist in drafting responses to inquiries from Congress and other agencies. The SP shall prepare, assist with the delivery, and maintain a record of briefings and presentations.

3.1.1 Policy Development

The SP shall assist in the drafting and implementing of IT policy, directives, manuals, orders, procedures, SOPs and guidelines as required by the DGR and submit them for approval and dissemination. The SP shall review, critique and provide recommendations to draft policy, directives, manuals, orders, procedures, SOPs and guidelines.

3.1.2 Strategic Planning

The SP shall provide input to the development of Departmental and supporting IT Strategic Plans. The SP shall assist in the development and submission of the IT Strategy to the DGR for approval in accordance with DOE directives and policies. In addition, IT Standards shall be updated accordingly. Task assignments may include assisting the Program Offices with efforts to develop and implement a Department-wide information architecture program and to develop guidelines and processes to ensure proper integration between the architecture, the Department's IT investment management process, and its cyber security program.

3.1.3 Enterprise Architecture

The SP shall, in accordance with approved IT Strategy, update and submit the Enterprise Architecture to the DGR for approval. In addition, IT Standards shall be updated accordingly. The SP shall ensure compliance with OMB Circular A-130, the Clinger-Cohen Act, and other directives as applicable. The SP shall work within the FEA reference models to ensure cross-agency analysis and the identification of duplicative investments, gaps, and opportunities for collaboration within and across Federal Agencies. Activities include, but are not limited to: promoting and implementing standard architectural practices; establishing enterprise architecture aligned with the Department's strategic goals facilitating an information exchange; ensuring the interoperability of business practices, systems and technologies; and providing a framework for corporate systems modernization.

3.1.4 Capital Planning and Investment Control

The SP shall perform IT capital planning and investment control activities in accordance with the IT Capital Planning Process. The SP shall perform work at the direction of the DGR in response to business needs. Activities may include, but are not limited to, assisting the Program Offices and Field Sites with efforts to develop and execute program-wide or enterprise-wide IT capital planning, as well as investment management guidelines and procedures. The SP shall provide expert consultation as well as knowledge of Government and industry best practices. The SP shall provide support activities to include, but not limited to, developing Exhibit 300's: Capital Asset Plan and Business Case, developing Exhibit 53's: Agency IT Investment Portfolio, developing supporting documentation, fact-finding, cost analysis, efficiency studies, and workload modeling, which may cut across all activities.

3.1.5 Resource Management

The SP shall perform resource management activities at the direction of the DGR. Task assignments may include, but are not limited to, assisting with efforts to: analyze and track budget expenditures; support IT budget process; implement automated financial systems; track and coordinate resource management; records management; and information systems efforts that support the implementation of DOE and other IT Management related regulations. The SP shall develop a strategy that recommends the proper allocation of human capital and funding for specific or defined tasks for particular periods of performance under the scope of the contract. This process produces the individual task management plans, to be submitted to the DGR for review and approval.

3.1.6 Procurement Actions

The SP shall provide or assist as required in the procurement of IT products and services, to include but not be limited to, hardware, software, firmware, materials, leases, Internet services, and licensing and maintenance agreements. Procurement activities may include, but are not limited to, researching products and services, developing and validating specifications, developing the procurement package, and

verifying the receipt of procured items. All such effort shall be defined in the approved task management plan and addressed as Other Direct Costs (ODC)

3.1.7 Special Projects

The SP shall provide expert assistance as directed in aiding the Government when Special Projects arise. Examples of Special Projects include, but are not limited to, Knowledge Management; i-Manage; e-Gov and ad hoc projects as the requirements are identified by the DGR.

3.2 Systems Development & Engineering

The following subsections detail specific SP responsibilities pertaining to systems development and engineering within DOE, including sensitive, classified and unclassified information systems. The SP shall provide expert consultation and perform work at the direction of the DGR in response to task assignments. Systems development and engineering tasks and sub-tasks are likely to include, but not be limited to, application development, modernization and enhancement, software engineering activities, configuration management web site development, and web site maintenance.

3.2.1 Application Development & Software Engineering

The SP shall provide services including, but not limited to: full life cycle software engineering support to a wide variety of systems (mission systems) that support the day-to-day business functions of various components of DOE. The SP shall provide IT development and support services to various software applications and data warehouses that support a variety of organizational and cross organizational functions.

All work performed must conform to the requirements of the Clinger-Cohen Act or other applicable DOE Orders, DOE Corporate IM Guidance, DOE Methodology, OMB Circular A-130, and the Joint Financial Management Improvement Program (JFMIP) and other applicable guidance. The SP shall identify the maturity level of the work being performed using the SEI/CMM. The SP shall adhere to the CMM level specified by the DGR for each sub-task order. These systems may be developed or enhanced using any combination of the following tools: COTS/GOTS products, and Database management software supplemented with custom code and/or high level programming languages as approved by DGR.

Existing applications shall be modified or enhanced per customer requirements as directed by the DGR to accommodate hardware, software, requirements changes, or software problems. DOE retains the right to acquire new systems and enhancements to existing systems, outside this Contract, to ensure the best value for the Government. The SP shall turn over all licenses, source codes, products and ownership to the Government at the end of each task assignment or contract, whichever arises first. The SP shall comply with Department of Defense (*DOD) 5200.28 STD: DOD Trusted Computer System Evaluation Criteria* when sanitizing IT equipment.

3.2.2 Web Site Development and Maintenance

The SP shall be responsible for the administration and maintenance of existing web sites within DOE, to include but not be limited to: verification of hyperlinks; implementation of new technologies as they become available (e.g., Multimedia, Streaming Technologies & Active Server Pages); adherence to existing Federal regulations (e.g., Section 508, OMB Privacy and Security). The SP shall assist DOE with various Government-wide initiatives, to include but not be limited to, Web Council and e-Gov. The SP shall respond to and implement inter-agency and other Federal requests and mandates for changes to existing web sites. The SP shall perform research and provide analysis about emerging technologies including, but not limited to, metadata, portals, and others as the need arises.

The SP shall be responsible for the development, administration and maintenance of new web sites within DOE as requested. This shall include but not be limited to, defining and developing of requirements (user and business); conducting testing; implementation; user training (on-site or remote); adherence to DOE EA Guidelines; database design, and maintenance, when applicable.

3.3 Information Technology Operations Support

The following subsections detail specific SP responsibilities pertaining to Operations Support within the DOE organization including sensitive, classified, and unclassified information systems. The SP shall be responsible for end-to-end operation of the network, including, but not limited to: IT facilities management & IT physical security; telecommunications/network engineering services; network administration; network configuration, installation, maintenance, repair and upgrades; firewall management and maintenance; server platform administration; server installation, maintenance, repair and upgrades; system back-ups and restores; applications system administration; disaster recovery; inventory control; maintenance and service agreement management; audio, video, and web conferencing; user support/help desk; workstation management; wireless services; voice and data services; spectrum management; classified information programs and surveillance systems. The SP shall be responsible for configuration management as it relates to the aforementioned activities. The SP shall be responsible for researching, testing and making recommendations for new hardware and software technologies as it relates to the business of DOE. The SP shall be responsible for ensuring that 'new' software introduced to the network meets all applicable guidelines and will work in the current operating environment.

3.3.1 IT Facilities Management & IT Physical Security

The SP shall work with administrative services, to ensure that facilities in use by the various IT department(s) have the proper power, heating, cooling, ventilation, lighting, space management, construction, security, and maintenance as appropriate for the various sites. The SP shall ensure that a backup and recovery strategy is in place and properly tested. Examples of areas to be considered include, but are not limited to, server rooms, switch closets, Local Area Network (LAN) rooms, and Network Communication Centers. The SP shall prepare, update, and maintain drawings of the various IT Facilities and other facilities for the purpose of configuration management, security, fire, safety, and physical planning. The SP shall provide a common repository of information regarding configuration management on all hardware and telecommunications equipment within the various IT Facilities' physical plants. The SP shall provide analytical work including research and planning documents to support facilities work to be performed for the various locations included under this contract. The SP shall plan and coordinate non-emergency outages affecting service areas. This includes, but is not limited to: creating timely notification of outages; maintaining physical security requirements and documents as deemed appropriate by the DGR; and maintaining both physical and logical drawings of the processors, peripheral equipment, and their connectivity. The SP shall coordinate all Configuration Change Proposals (CCP) with Change Control Boards (CCB) or the appropriate personnel as it relates to IT services. The SP shall also perform administrative management support functions as directed by the DGR.

3.3.2 Network Administration

The SP shall perform networking activities pertaining to the DOE's facilities. These responsibilities include, but are not limited to: consulting with customers; gathering customer requirements; problem identification; capacity planning; network optimization and tuning; and meeting certification and accreditation requirements. The SP shall be responsible for providing identity management of network access to authorized personnel; providing a secure environment for applications to reside; designing and implementing networks; providing remote access; network configuration management; establishing a testing environment, installation, maintenance, repair, and upgrades of all hardware, firmware, software, and associated equipment that is installed as part of the network within DOE sites.

3.3.2.1 Network Configuration, Installation, Maintenance, Repairs, and Upgrades

The SP shall perform network functions to ensure access to network resources. The SP shall identify customer and technical network requirements and prepare an analysis for capacity utilization assessments in accordance with DOE guidelines for DGR approval. The SP shall create and maintain documentation to support the testing, installation, and operation of networks. The SP shall be responsible for end-to-end network operations and maintenance services to ensure connectivity of all installed networks related to DOE sites. Network functions include, but are not limited to, firewalls management and maintenance; server administration; server installation, repair maintenance and upgrades; system back-ups and restores;

applications system administration, disaster recovery planning and execution, and cabling Systems installation, maintenance and upgrades. The SP shall coordinate all CCPs with CCBs or the appropriate personnel as it relates to IT services.

3.3.2.2 Firewall Management and Maintenance

The SP shall be responsible for engineering, architecture, management, planning, implementing, maintaining, repairing, upgrading, configuring, and documenting all firewalls to ensure the DOE confidentiality, integrity, security, availability, and authenticity through the Internet/Intranet. The SP shall respond to cyber security needs and requirements, both emergent and as identified in the Cyber Security Program Plan (CSPP) and other directives/mandates. The SP shall maintain and manage firewall components and configuration; and maintain the security posture of the firewall components on a regular basis through the use of security tools. The SP shall monitor the firewall on a daily basis for penetration attempts to evade security and maintain incident reports of such events. The SP shall notify the Computer Incident Advisory Capability (CIAC), all Program Offices, and Field Sites of any security incidents that occur involving a specific site and/or IT asset. The SP shall coordinate with other DOE contractors, as applicable, to discuss firewall implementation needs and configuration issues. The SP shall implement approved firewall exception requests, alerting Department Officials of potential problems with an approved request prior to implementing, and notifying the requestor of the firewall exception when the exception is implemented or not approved. The SP shall interface with DOE personnel, when appropriate.

3.3.2.3 Server Administration

The SP shall manage all production, test, and development servers. Server administration includes, but is not limited to, account management, monitoring and auditing system logs, back up and recovery, security, managing operating systems, and storage management. The SP shall perform all non-emergency disruptive work on servers during non-business hours or at the direction of the DGR.

3.3.2.4 Server Installation, Maintenance, Repairs, and Upgrades

The SP shall be responsible for the complete installation, testing, problem determination, maintenance, repair, configuration, and documentation of all hardware, firmware, software, and associated equipment that is installed as part of a server. The SP shall ensure that server operating systems will be maintained at the level dictated by the enterprise architecture. The SP shall meet certification and accreditation requirements. The SP shall identify server requirements and prepare a systems analysis in accordance with DOE guidelines. The SP shall create and maintain documentation to support the testing, installation, and operation of servers. The SP shall coordinate and validate changes with application owners. The SP shall coordinate all CCPs with CCBs or the appropriate personnel as it relates to IT services. The SP shall ensure that all non-emergency disruptive maintenance, repairs and upgrades are performed during non-business hours or at the direction of the DGR.

3.3.2.5 System Back-ups and Restorations

The SP shall perform system back-ups and restore-functions to ensure data availability. The SP shall demonstrate and test back-up and restore reliability. The SP shall ensure the restoration and/or reproduction of current and historical systems, applications, and data in accordance with DOE management directives and requirements for data recovery. The SP shall follow all DOE directives and requirements regarding off-site storage, including disaster recovery requirements.

3.3.2.6 Application Systems Administration

The SP shall provide all support required to maintain and provide reliable access to application systems. This support includes, but is not limited to: hosting the application and ancillary software (databases, etc.) on servers, which provide adequate bandwidth and response time for users; and providing adequate network connections, possible n-tier systems where applicable, and web access interfaces where required. The SP shall perform these duties, configuration management, and other requirements listed herein in accordance with the instructions as noted in the PRS, or as otherwise directed by the DGR, who will

determine requirements, adequacy, and reliability. Application upgrades and patches will be installed in a timely manner consistent with change control requirements. Day to day operational processing and fixes shall be performed in a manner which meets the DGR determined reliability requirements of the users, system uptime, and the business needs of the organization. The SP shall provide access control in order to provide proper rights and privileges to approved users for specific applications. The SP shall remove rights and privileges for terminated employees within specified timeframes, and maintain access logs.

3.3.3 Emergency Preparedness

The SP shall support all emergency preparedness activities to include disaster recovery planning, and execution, and development of the Continuity of Operations Plan.

3.3.3.1 Disaster Recovery Planning and Execution

The SP shall create, execute, obtain approval for, update, maintain, provide audit support, and test Disaster Recovery Plans for all major IT systems-including general support systems and corporate and critical applications as defined by the DGR. The SP shall conduct and participate in test exercises as required by applicable Disaster Recovery Plans.

3.3.3.2 Continuity of Operations

The SP shall adopt existing and/or create, execute, obtain approval, update, maintain, and test Continuity of Operations Plans (COOP) for all major IT systems, including general support systems and major applications. The SP shall integrate all IT COOPs into appropriate higher-level COOPs. The SP shall conduct and participate in test exercises for the DOE COOPs.

3.3.4 Inventory Control

In accordance with DOE standards, the SP shall maintain and supplement the existing property management systems, policies, and procedures to ensure that inventories of Government Furnished Property (GFP) are properly maintained and updated for all IT related items to include, but not limited to, hardware, software, licensing agreements, maintenance contracts, wireless devices, and spare parts in accordance with local policies and procedures. The SP shall identify and support the DGR in the disposal of excess GFP. For approved excess GFP this includes ensuring timely sanitation in accordance with DOD 5200.28 -STD and transfer of sanitized surplus equipment for disposal in accordance with local policies. When applicable, the SP shall coordinate IT inventory efforts with physical inventory personnel to ensure compliance.

3.3.5 Maintenance, Support and Service Agreements Management

The SP shall support management of maintenance and support agreements for hardware and software as specified by the DGR. The SP shall ensure that all such agreements are registered with the provider in the name of DOE. The DGR shall appoint DOE administrator(s) for these agreements. The SP shall support management of service agreements including, but not limited to, commercial or third party service providers, Enterprise Resource Planning (ERP), and pre-paid consulting services. Management activities shall include, but not be limited to, ensuring continuity of coverage; ensuring adequacy of coverage; ensuring agreement information is available, complete, and accurate; and analyzing cost effectiveness.

3.3.6 Audio, Video, and Web Conferencing

The SP shall provide maintenance for video room operations, systems design, engineering, installation for new and/or relocation of video systems and network/Integrated Services Digital Network (ISDN) equipment for the DOE users. The SP shall provide video-broadcast and reception services over satellites leased for Government use. The SP shall use both new and existing hardware and software packages as directed by the DGR.

The SP shall provide video production services, both recording and taping, as needed. The SP shall provide engineering and configuration management of the ISDN and coordination with commercial

carrier as necessary for repair and new installation of additional access from FTS2001, successor contracts, and a local carrier.

The SP shall perform traffic studies of the ISDN each month and make appropriate recommendations according to capacity needed in order to provide this service. The SP shall make the results of the studies available to the DGR upon request. The SP shall provide all technical interfaces with other vendors and serve as the point of contact for ISDN/video projects at the various DOE locations.

The SP shall maintain a scheduling function that supports the various program offices and numerous field sites, nationwide, and provide analysis of the usages by organization on a monthly basis. The SP shall provide training to users on all video equipment and how to make calls to any location within the DOE video community as well as international calls. Examples of work that will be performed as part of the scheduling function includes, but is not limited to inquiries, cancellations, and confirmation in support of video events for Satellite Broadcasts and video teleconferences. The SP shall provide mobile uplink service as required. The SP shall advise DOE about upgrades or changes in configuration of the Video Network to ensure a highly reliable and cost effective system. The SP shall ensure that available services are adequate and meet Federal and general commercial standards as directed by the DGR.

3.3.7 User Support

The SP shall be responsible for Customer Relationship Management (CRM), which shall include, but not be limited to, pre-service activities, during service activities and post-service activities, customer surveys and follow-up, and liaison with the customer. The SP shall provide user support as defined at the task level, to include, but not be limited to, help by telephone, remote control, and/or support at the desktop/problem area. The SP shall perform new user set-ups, account termination, the establishment of e-mail and messaging accounts as well as telecommunication services, and the set up of peripheral/portable devices. Equipment identified for disposal shall be processed in accordance with *Section 3.3.4: Inventory Control.* The SP shall perform problem resolution according to the timelines set forth in the PRS. The SP shall manage desktop hardware and software assignments and address warranty problems. The SP shall provide environment orientation, overview training, and group training on an as needed basis. The SP shall record, analyze, maintain, and prepare and submit required reports regarding problem resolution occurrences and trends. The SP shall provide self-help training aids (e.g., tips & tricks, FAQ's) content for recurring problems as needed or required.

3.3.8 Workstation Management

The SP shall perform workstation management to ensure the proper planning, design, implementation, deployment, administration, maintenance, repair, modification, final disposition, day to day operation and upgrade to operating systems, software applications, and hardware utilized on user workstations. Activities include, but are not limited to: providing and maintaining a DGR approved refresh rate; performing PC adds, moves, and changes; loading clients; central management and remote management of desktops; and providing loaner equipment. The SP shall research, apply, distribute, and document desktop patches and service packs.

3.3.9 Wireless Services

The SP shall install, operate, maintain, repair, upgrade, configure, and document all wireless technology required to meet the business needs of the organization. Technology includes, but is not limited to, cellular telephones, radio frequency communication (conventional and trunking), microwave, satellite links and bi-directional satellite links, Personal Digital Assistants (PDA), paging systems (advanced messaging), wireless LANs, repeaters and all associated support equipment that completes the wireless LAN system. The SP shall provide engineering services during the planning and budget formulation phase, to be followed through to Project Management and final inspection of a wireless telecommunications and/or networking systems. The SP shall track and review costs and billing associated with wireless services.

3.3.10 Voice and Data Services

The SP shall plan, coordinate the installation, maintenance, repair, upgrade, configuration, operation, and documentation of the voice, fax, and data services, telephone switches and voice mail systems, E-911 system, and telephone interconnect networks. The equipment may include, cable plant (analog/digital, fiber optic, and copper for voice and data); and data network connectivity, to include but not limited to T1, T3, and ISDN lines, and external dial tone. The SP shall provide engineering design support, technician support, and project estimation support and shall conduct infrastructure upgrades to software, firmware, and equipment. The SP shall maintain and provide when requested the cable plant records and the Title III engineering drawings for new systems.

As applicable, the SP shall monitor, operate, and maintain a telecommunications management system for customers, including, but not limited to: conducting customer user units moves, adds, and changes; updating the operator and directory service call detail reporting; performing trouble resolution, billing, work order logging and dispatch; and facilitating the moves, adds, and changes.

3.3.11 Spectrum Management

The SP shall perform all activities related to Spectrum Management. The SP shall develop a spectrum strategy for local, nationwide, and worldwide system utilization. The SP shall maintain the classified Government Master File (GMF) to assist in the corroboration and review all new proposals and procurements for Government-authorized radio communications equipment. The SP shall maintain a database for all licensed and non-licensed radio services and prepare and review for regulatory compliance all spectrum requirements prior to preparing and submitting spectrum certifications and radio frequency requests to Headquarters.

The SP shall renew frequency licenses, including continued justification for the spectrum. The SP shall work with the system engineers to develop the Spectrum Management requirements and submit the appropriate applications to seek National Telecommunications and Information Administration (NTIA) and Department of Commerce (DOC) approval for frequency channel and bandwidth usage. The SP must exhibit the ability to do spectrum analysis to determine on-channel and co-channel (intermodulation) frequency interference and propagation analysis. The SP shall take measures to ensure spectrum efficient technologies are used and spectrum is shared whenever possible. The SP shall process all requests through the NTIA for Spectrum dependent equipment. The SP shall act as a liaison between the field offices of DOE and the Department of Commerce, regarding all requests for spectrum management.

3.3.12 Surveillance Systems

The SP shall provide support for the planning, implementation, maintenance, repair, upgrade, configuration, operation, and documentation of alarm, public address, and electronic security systems installed in DOE facilities in accordance with 40 CFR 194 and any DOE Safeguards and Security Directives. This work includes, but is not limited to, the design, installation, maintenance, and repair of alarms and related electrical circuits, maintaining and testing access control systems, maintaining and testing fire alarm circuits and fire suppression systems, and testing video monitoring systems. The SP shall ensure that surveillance data is available and archived in accordance with NARA standards or as directed by the COR.

3.4 Cyber Security

Cyber Security is the protection of information technology investments (e.g. information systems and telecommunications systems) and the information within or passing through them from unauthorized access, use, disclosure, disruption, modification, or destruction in order to ensure the integrity, confidentiality, and availability of DOE IT systems. Integrity means guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. Confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information. Availability means ensuring timely and reliable access to, and use of information and information systems.

The SP shall provide Cyber Security for DOE by complying with DOE O 205.1, DOE Cyber Security Management Program, dated March 21, 2003 and any other applicable security regulations and policies. The SP shall ensure that all sub-contractors are aware of and comply with the requirements maintained in DOE O 205.1. The SP shall employ a variety of methods to ensure that Cyber Security is being accomplished. These methods include, but are not limited to, cyber resource protection; risk management; program evaluation; cyber security plan development and maintenance; auditing tools; and network intrusion detection tools.

3.4.1 Cyber Resource Protection

The SP shall protect all DOE unclassified and classified information and information systems under its management. The SP shall control all information systems at all times commensurate with the risk and magnitude of harm that could result to national security interests and DOE missions and programs resulting from a loss of confidentiality, availability, or integrity of the information or systems. The SP shall serve as senior network security technical advisor, and perform a detailed examination of the security management and monitoring procedures/resources required to keep the Department in compliance with Federal cyber security directives and best business practices.

The SP shall provide network vulnerability scanning services and analysis as well as track and report configuration and vulnerabilities of SP supported systems, corrective actions taken, and vulnerability mitigation. The SP shall establish, implement, and maintain the following controls: limit and control outside visibility to DOE systems; limit and control access to the same systems; limit and control network interfaces across security boundaries, and monitor and report anomalous, security related (network) activity.

The SP shall provide cyber and network support services 24 hours a day, seven days a week that include, but are not limited to, responding to real or potential security events; responding to Federal data calls or other mandated reporting requirements; providing after-hours security support for the DOE networks and all associated Program Offices and field sites.

The SP shall oversee response(s) to all incidents involving malicious or suspicious code to include, but not be limited to; viruses, Trojan horses, worms, and macros. The SP shall respond to malicious attacks, provide technical advice when required, and collect incident tracking information. The SP shall maintain a database of all pertinent information relating to malicious code encounters and incidents including, but not be limited to, virus, user, organization, location, source, affected media, and whether the incident was internal or external to DOE. The SP shall coordinate with other Federal elements and vendors as needed.

The SP shall implement anti-viral tools as necessary including, but not limited to, configurations and dissemination mechanisms, filtering, blocking, and auditing. The SP shall provide senior expertise, guidance, resources, and analysis for organizational and enterprise virus protection audits as required. The SP shall develop and maintain mechanisms for distribution of anti-viral software to virus response staff, system administrators, and users both at the desktop and home. The SP shall also provide reports of virus encounters on a monthly basis to the DOE CIAC, Virus Bulletin, and others as necessary. The SP shall ensure that all virus definitions for anti-virus software are kept current, within 24 hours of release of the new definitions either through manual or electronic means.

3.4.2 Cyber Security Planning

The SP shall develop and maintain approved CSPPs in accordance with the applicable Program Cyber Security Plans (PCSP). The DOE will provide the SP with the PCSP and or CSPP. The SP shall submit plans for review and update when operational considerations (e.g., risks, threats, cyber assessment configurations, vulnerabilities, or DOE cyber security directives) change significantly, or as required by relevant DOE Orders. The SP shall provide CSPPs on an annual basis.

3.4.3 Cyber Risk Management

The SP shall facilitate or lead risk analysis and implement a DGR approved risk management approach for protecting information and information systems as described in the CSPP. The SP shall document the

risk management process, and this process must be used to support informed decisions related to the adequacy of protection, cost implications of further enhanced protection, and acceptance of residual risk. The SP shall complete self- and peer-assessments as required by DOE to ensure it meets DOE's requirements.

SECTION 4: KEY PERSONNEL

4.1 Personnel

Key personnel shall be identified with the SP's proposal and will be incorporated herein at the time of the award. For all task assignments, at the time of the award, the SP shall identify key individuals that will be assigned to support each functional area at all times under this PWS. In the event of key personnel departures, the SP shall ensure support for all DOE requirements until permanent replacements are available. These replacements are required within 20 business days after the departure of a key individual. Final approval of changes to key personnel must be approved by the DGR.

4.2 SP Program Manager

The SP shall provide as key personnel a SP Program Manager (PM) and designated alternate(s), who shall be responsible for the performance of the work. The designated alternate(s) shall act for the SP in the absence of the PM. The names of these key personnel shall be included in the proposal.

The PM shall be the SP's authorized representative for the technical and administrative performance of all services required under this PWS. The PM shall be the first Point of Contact (POC) for contractual or administrative questions or difficulties that arise related to this PWS. The PM shall be the primary point through which communications, work assignments, and technical direction flow between the Government and the SP. The DGR shall be the SP's first POC in the Government.

The PM shall be available during normal hours of operation to plan, direct, and control the overall management and operational functions specified herein. The PM shall provide the necessary level of contract management and administrative oversight to achieve the quantitative and qualitative requirements of this PWS.

The PM or designated alternate shall be available within thirty (30) minutes during normal work hours to meet with the DGR, in person or as specified by the DGR, to discuss problem areas. After normal working hours, the PM or designated alternate shall be available within sixty (60) minutes after notification to coordinate any necessary actions.

SECTION 5: GENERAL REQUIREMENTS

5.1 Service Provider Management Requirements

SP responsibility shall include all planning, programming, administration, management, and execution necessary to provide the specified services. The SP shall ensure that all work efforts meet the requirements of Contract provisions and PWS *Section 3: Performance Objectives and Measures*, the PRS (see *TE 3-2: PRS*), or in applicable referenced documents, directives and regulations.

The SP shall perform all related administrative services required to perform work including, but not limited to: material requisitioning, Quality Control (QC), financial control (cost control/savings), status/tracking reports, and correspondence. The SP shall also maintain accurate and complete records, files, and libraries of documents to include, but not be limited to: federal, state, and local regulations, codes, laws, technical manuals, and manufacturer's instructions and recommendations, which are necessary and related to the functions being performed. The SP shall compile historical data, prepare required reports, and submit information as specified in *TE-3-3: Required Reports*. The SP shall assume total responsibility for all requirements stated herein on the Contract start date; this may include the management of all existing IT contracts as well as sub-contracts. The SP shall support DOE during audits and inspections, and provide support and responses to audit and inspection items (internal and external).

5.2 Service Provider Personnel

SP personnel shall follow all relevant guidelines as published by the Government.

5.2.1 Service Provider Employees

SP personnel shall meet relevant DOE security requirements as identified in *TE 5-1: Security Clearance Requirements.* The SP shall provide a sufficient number of personnel possessing the skills, knowledge, and training to satisfactorily perform the services required by this PWS for each specific functional area. For SP training responsibilities, see *Section 5.2.4 Employee Training.*

5.2.2 Employee Data

The SP shall maintain a sortable on-line employee roster accessible to the DGR of individuals who will perform work under this PWS. The roster shall include the data specified below. The roster shall be updated for each change within five (5) working days of its occurrence. The SP shall also provide a quarterly personnel report to the DGRs as directed in *TE 3-3: Required Reports* with the following information:

- Employee Name
- Labor Category/Job Title
- Government/Contractor/Sub-Contractor Name
- Size of Business (Large, Small/Small Disadvantaged, etc.)
- Organization Code Being Supported (IM-12, SO-33, etc.)
- Functional area of the Contract/Task Assignment (TA)
- Sub-Task Assignment Number being supported
- Security Badge Level (Q, L, Building Access Only (BAO))
- Phone Number
- Facsimile Number
- Site Location/Address
- Room Number
- Mail Stop
- E-mail address

In addition, DOE currently maintains an integrated electronic directory which includes DOE Federal, other Federal, and contractor personnel. Employees requiring services from DOE (e.g. a user ID, a badge, an e-mail account, etc.) will only be provided the requested service if they are in this integrated directory. To accomplish this, the SP shall have employees requiring DOE services provide information to the

directory about their employees. The SP shall provide data as new employees are assigned to Task assignments and also remove employees from the directory upon departure.

5.2.3 Organizational Chart

The SP shall submit an Organizational Chart showing the SP's functional responsibilities with the Employee Locator Log/Directory.

5.2.4 Employee Training

The SP shall be responsible for all new and recurring training of SP personnel in such a manner as to ensure all tasks required by this PWS are performed properly. The Government may provide training for DOE proprietary requirements.

The SP shall conduct or provide to their employees detailed instruction on Government policies and regulations in areas such as employee conduct ethics, safety, security, health, fire prevention, and the environment as they pertain to the operations specified in this PWS. The SP shall develop, implement, and maintain written guidelines or standard procedures necessary for effective accomplishment of PWS requirements. The SP shall comply with all Privacy Act regulations governing personal and private information.

5.2.5 Employee Conduct

The SP and its employees shall comply with all Federal, state, local laws, applicable policies and mandatory DOE conduct standards and regulations. The DGR may require the SP to remove from the job site any employee working under this PWS for reasons of misconduct, security infraction, or employees found or suspected to be under the influence of alcohol, drugs, or any other incapacitating agent. The SP shall maintain provisions for the immediate removal of employees for misconduct, or other causes prejudicial to the maintenance of health, welfare, morale, or security of DOE and populace thereof, and shall exercise these provisions.

5.2.6 Access Requirements

The Government has the right to restrict and control access to its facilities, property, and data, including those that are identified in this PWS. Access privileges will be tailored to individual SP personnel responsibilities. The Government will be the final authority in determining access privileges. The Government's exercise of its right to grant and revoke access by 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 SP, and regardless of whether said individual(s) are precluded from performing work under the PWS.

5.2.7 Coordination

SP personnel shall coordinate with Government personnel and other Government contractors performing required services in areas associated with the requirements of this PWS. Some examples include, but are not limited to: personnel performing security functions, audits, inspections, delivery services, construction, and telecommunication services. The SP shall provide the DGR with a copy of any SP/Sub-contractor insurance policy or license associated with non-governmental facilities per request of the DGR. The SP shall schedule operations so as to minimize interference with other Government work.

The Government will facilitate initial contact between the SP and other contractors performing work for DOE. The SP shall provide all further required coordination with other contractors for any task specified in this PWS that relates to or impacts on any other contracted work. The SP may be responsible for support services to other contractors within the scope of this PWS as required by the Government.

The SP shall notify the DGR of unresolved disputes in receiving support from or providing support to customers or other contractors within two (2) business days from the time the dispute occurs, unless otherwise specified in *Section 3: Performance Objectives and Measures.*

5.3 Records Maintenance and Reporting

The SP shall create and maintain files (e.g. records, reports, and logs) documenting the processing of work and associated information. Access to this information shall be governed by Federal laws, regulations, and the direction of the DGR.

5.3.1 Records Maintenance

The SP shall make files available to the DGR upon request within five (5) business days of receipt of the request. The Government retains ownership of all files. The SP shall provide long-term storage of inactive files and destroy obsolete files in accordance with National Archives and Records Administration (NARA) regulations The SP shall maintain all records including files, documents, desk guides, and working papers provided by the Government and/or generated for the Government in performance of this PWS become and remain Government property. These records shall be maintained in a format approved by the DGR. In the event of default, or non-performance, the Government will have access to records in order to ensure mission support is not interrupted. All such records shall be turned over to the Government at the completion or termination of the Contract.

5.3.2 Criteria

The SP shall respond to DOE requests for information, including scheduled (programmed) and ad hoc (un-programmed) requests, from the DGR. The SP shall refer all requests for support to the COR if received from other Government personnel prior to responding. The SP shall submit to the DGR programmed and un-programmed information, subject to Government review for adequacy, utilizing the following criteria:

- Complete: To include all information
- Accurate: Factual and correctly tabulated data
- Preparation: In accordance with applicable publication, or other specified format
- Authorized: Name and signature of PM
- Timely: Provided within the specified time frames
- Distribution: Provided to the specified recipients

5.3.3 Programmed Reporting Requirements

The SP shall report all work accomplished under the PWS and shall furnish the workload data to the DGR in letter and electronic format by close of business (COB) on the fifteenth calendar day of the following month. The workload data shall be in a format compatible with Government accounting systems and subsystems (as they may change from time-to-time) and workload analysis automated information systems (AIS) where such exist. The workload data shall reflect all work accomplished by the SP's project staff directly expended with applicable costs attributed to appropriate tasks. Functional area workload shall be severable by task or subtask. The workload data shall be subject to review and comment by the DGR and shall be updated as required.

The SP shall furnish all recurring contract data and information as listed in *TE 3-3: Required Reports*.

5.3.4 Ad-Hoc Reporting Requirements

Upon notification by the DGR, the SP shall provide management and technical information including, but not limited to: technical evaluation of suggestions, input for staff studies, fact sheets, audits, congressional inquiries, one-time reports, material, equipment, facilities, property inventories and other listings, equipment maintenance records. Recommendations for amending, revising, or originating Government regulations or policies within the scope of this PWS information requested by Government personnel performing official duties, to include monitoring PWS compliance. Responses to Government and other contractor personnel conducting information and communication systems site surveys, information systems fielding, and communication engineering and construction as required by the Government are included.

5.3.5 On-Line Tracking Report

The SP shall provide an on-line tracking report that provides the DGR a current record of all financial information and transactions from time of award to contract/task assignment closeout. This should address total costing including obligated or de-obligated funding associated with each task assignment and any new funds supporting task modifications, funding amount that is invoiced for Labor or Services, ODC's, any Incentive/Award Fees (if applicable) by task assignment, and/or Project level. Also the tracking system shall have the most current Contract/Task assignment Statement of Work and surveillance plan associated with the issued task assignment, and SP approved management plan. The level of detail required for this report is subject to change at the discretion of the DGR.

5.3.6 Access to Data and Information

The SP shall ensure that all generated technical records, reports, files, and other documentation are complete and made available to the DGRs during the performance of this PWS.

The SP shall not release any news (including classified and non-classified information, photographs and films, public announcements, or denial or confirmation of same) or IT related information of any subject matter within this PWS or any phase of any program herein to the media or any other unauthorized individuals without the prior written approval of the DGR. The SP shall provide support to the CO for all Freedom of Information Act (FOIA) requests and refer FOIA inquiries to the CO.

5.3.7 Marking Proprietary Information

All records, files, reports, and data deemed proprietary by the SP shall be clearly marked accordingly. The Government will make the final determination of the appropriateness of proprietary claims by the SP.

5.3.8 Publications/Technical Library

The Government will initially establish a Technical Library to facilitate the solicitation process for all potential offerors. Following Contract start, the SP shall maintain the Technical Library, including all publications, data, exhibits, and other information provided in accordance with DOE laws and regulations. The Technical Library shall be updated as required to ensure that all information is current and accurate. The Technical Library shall be considered Government property and consist of information necessary to prepare a proposal excluding potential offertory proprietary information.

The Technical Library will contain copies of all Government-unique regulations and publications cited in this PWS. Regulations and publications are identified in *Section 3: Performance Objectives and Measures* and in *Appendix B: Technical Library.* The SP shall request through the DGR, supplements, updates, and other publications requirements in direct support of this PWS. The Technical Library may contain classified information and access to this information is governed by applicable laws and regulations.

The SP shall become acquainted with and comply with all Government regulations as posted, or as required by the DGR. Regulations, manuals, and technical documents applicable to this PWS are listed in *Appendix B: Technical Library*.

The potential offeror/SP shall utilize the Technical Library as follows:

- Procure commercial publications, including manufacturer's manuals, necessary to perform under the terms of this PWS
- Comply with all facility regulations specified in Appendix B
- Order, follow-up, and ensure timely distribution of updates and other publication requirements; publications shall be kept current and maintained in accordance with applicable DOE rules and regulations.

The COR will furnish, upon request, a copy of existing and available facilities and network diagrams that will be essential to perform the services specified in the PWS. When discrepancies are found in network diagrams and other publications, the SP shall notify the COR of possible changes.

The SP shall obtain commercial publications required in the performance of this PWS with the approval of the DGR.

The DGR will make an initial supply of forms available to the SP at Contract start date. Samples of standard Government forms required for the fulfillment of this PWS will be available for SP examination in the Technical Library. However, these forms and logs are subject to change periodically, and the SP is responsible for keeping track of form changes.

5.4 Security

5.4.1 General

The SP shall identify a single point of contact to serve as the SP Security Officer and provide this information to the DGR within ten (10) calendar days of Contract award. Notification of any changes in responsible individuals shall be given to the DGR no later than fifteen (15) calendar days prior to the change. The SP shall be in compliance with DOE Security Orders as listed in *Appendix B: Technical Library* for all security-related matters.

Compliance by the SP shall be mandatory for security access requirements to restricted areas that include, but are not limited to, communication centers, nuclear facilities/related sites, computer centers, and research and development areas. The SP shall clear requests for work in restricted areas with the Government's Security Officer. A list of Government security POCs will be furnished to the SP prior to the Contract start date.

5.4.2 Personnel Security Clearances

SP personnel are required to obtain security clearances in accordance with *TE 5-1: Security Clearance Requirements*. DOE has final authority on determining an individual's security clearance eligibility. The SP shall submit requests for security clearances for staff. The SP shall, prior to submitting an employee for security clearance, perform a preliminary criminal and financial background check of prospective employees who may be performing services defined in this PWS to assure that the employee being offered the position will be able to obtain the required DOE security clearance.

All employees may be required to attend the annual Computer Center Escort training and other security related training as required.

5.4.3 Personnel ID Requirements

SP personnel shall wear an ID security badge issued by DOE at all times while on-site, as implemented by facility regulations. The SP shall ensure that employees return these security badges upon termination or reassignment to another location and notify the appropriate DOE security office that the employee will no longer require on-site access. The SP shall update the Employee Roster with any changes.

DOE has final authority on determining an individual's security clearance and site access eligibility. All personnel assigned to IT functions as described in this document must be U.S. Citizens. The SP shall identify (on the SP Employee Roster) those employees who require access to restricted areas or classified information, and shall obtain and maintain the appropriate security clearances as identified in this solicitation.

5.4.4 Physical Security Plan

The Physical Security Plan shall be established in accordance with the requirements of DOE Headquarters and Field Organizations. The SP shall submit the Physical Security Plan to the DGR for approval within 30 calendar days after Contract award. The plan shall outline procedures to provide internal safeguards for the security of all GFP and all property in the possession of the SP for the performance of required services. The SP shall update the plan as changes occur and shall submit a copy of the proposed plan to the DGR for approval no later than 30 calendar days prior to the proposed effective date of the updated plan. The SP will be subject to unannounced physical security inspections by the DGR

5.4.5 Information Security Plan

The SP shall develop an Information Security Plan in compliance with DOE Headquarters and Field Organization regulations. This plan shall provide for the control of classified information related to handling and accessing classified information and control of all computer security and communications security utilized within the scope of this PWS. The SP shall submit the Information Security Plan to the Government for review 30 calendar days prior to Contract start date and implement the plan at Contract start date in all facilities.

5.4.6 Restricted Areas

The SP shall comply with procedures and instructions for restricted areas. Work performed in restricted areas shall be coordinated with the respective restricted area Government Security Officer. The Government has the authority to deny access to restricted areas.

5.5 Key Control

The SP shall establish and maintain on file a written Key Control Plan to ensure that keys or other access means (such as access badges, pass codes, biometric access, etc.) issued to the SP by the DGR are not lost, misplaced, or used by unauthorized persons. This Key Control Plan shall also include the names of individuals and the special access areas to which they are authorized by using their badge or other special access means. This plan shall be provided to the DGR for review 30 calendar days prior to the Contract start. The SP shall revise and implement the plan upon request from the DGR. The SP shall update the plan as required and as requested by the DGR. The SP shall maintain records as required by DOE regulations to ensure accountability of keys and authorized access.

Master/file keys for buildings will only be issued to SP employees performing services under this PWS. Building numbers or room numbers shall not be placed on master/file keys. Keys shall be coded so as to identify facilities, buildings or room numbers. The SP shall provide two (2) copies of the key inventories to the DGR within five (5) business days of the date of request. The SP shall not duplicate government keys unless authorized in writing by the DOE Physical Security Officer.

The use of Government keys or other access means issued to the SP by any person other than authorized SP employees is prohibited. The SP shall not permit entrance to locked areas to any person other than SP personnel engaged in performance of work in those areas without written authorization by the DGR. The DGR will have access to any Government-owned property under the control of the SP.

The SP shall report any occurrence of lost keys, lost badges, or unauthorized access to the DGR within 30 minutes of discovery of the loss or unauthorized access. The SP shall provide the DGR a written report by COB the next business day or as otherwise directed by the DGR. The report shall contain the key number, location(s) accessed by the key, date the key was discovered missing, name of person signing for the key, immediate risks and mitigation, and any other relevant details.

5.6 Other General Information

5.6.1 Certifications, Licenses and Permits

The SP shall obtain all necessary certifications, licenses, and permits required for performance of work and for complying with all applicable federal, state, and local laws and regulations. Such documents shall be kept on file and returned to the Government upon expiration or termination of the Contract.

5.6.2 Warranty Maintenance

Before the Contract start date, the Government will provide the SP with the records of all Government-owned property and equipment that is under warranty and used, managed, or supported under this PWS. The records will identify the item, the nature and expiration date of the warranty, and the name and location of the firm to contact about entitlement under the warranty. The SP shall provide the Government with copies of warranty records on any items of equipment or repair items to which the Government will take title or which will be installed on Government property. The Government will maintain a record copy of all warranties.

The SP shall monitor and track all Government-owned equipment falling under the maintenance responsibility of the PWS. The SP shall exercise existing manufacturers' commercial warranties on all Government equipment, including warranties on existing equipment, equipment replacements, and new equipment acquired under this PWS and by other contractors. The SP shall report to the DGR difficulties encountered in the enforcement of warranties and instances in which the costs of enforcement would exceed the benefits derived. The SP shall submit a warranty plan in line with the task assignments.

Existence of a warranty does not relieve the SP of his responsibility to perform work needed to prevent potential damage to personnel/property or to prevent unnecessary shutdown of facilities/functions. The SP shall inform the Government in writing of all warranty actions involving GFP.

5.6.3 Inspection by Government Agencies

The SP shall provide access to GFP and cooperate with visiting Government personnel conducting official inspection visits and surveys at the facilities. Inspection visits will be made by agencies including, but not limited to, the Office of Inspector General, General Accounting Office (GAO), Environmental Protection Agency (EPA), Occupational Safety and Health Administration (OSHA), and other DOE inspection organizations.

The SP shall notify the DGR of planned visits, investigations, or corrective actions required by federal, state, and local agencies. The SP shall notify the DGR by phone within 30 minutes of unannounced arrival of any agents of any regulatory agency at Government facilities operated by the SP.

The SP shall submit a written report to the DGR, by COB on the next workday following completion of an inspection/visit, to include the name(s), ID number(s), agency(s) of the inspector(s), reason for visit, and any remarks made during the visit. The SP shall include a copy of all reports received and, if samples or photographs are collected, examples of the samples provided or photographs taken. A statement signed by the SP validating their authenticity shall accompany samples.

5.6.4 Fraud, Waste and Abuse

The SP shall be responsible for maintaining proper conduct and good discipline within SP occupied work area. SP personnel shall be encouraged to be alert to and report all suspected situations of fraud, waste, and abuse, or other intentionally dishonest conduct against the Government observed during or in the performance of the contract provisions.

5.6.5 Hours of Operation and Government Holidays

The performance requirements established by this PWS shall be accomplished during normal work hours or as directed by the DGR. However, some requirements may require unique schedules to its mission requirement, and those hours will be assignment specific. Normal work hours are a range of hours established at each site. The days specified below are legal public holidays and other periods that are observed. If the holiday falls on a Saturday, the recognized federal holiday is the preceding Friday. If the holiday falls on a Sunday, the recognized federal holiday is the following Monday.

Holiday	Date
New Year's Day	1st day of January
Martin Luther King's Birthday	3rd Monday in January
Presidential Inauguration Day	Every 4 years (Washington, DC metro area only)
President's Day	3rd Monday in February
Memorial Day	Last Monday in May
Independence Day	4th of July
Labor Day	1st Monday in September
Columbus Day	2nd Monday in October
Veteran's Day	11th of November
Thanksgiving Day	4th Thursday in November
Christmas Day	25th of December

5.6.6 Disaster Recovery, Emergency Situations, and Special Events

Disaster Recovery support shall be in accordance with *Section 3: Performance Objectives and Measures*. Emergency situations (including, but not limited to, disasters of any kind whether natural disasters, accidents, or terrorist-related in nature) may necessitate the SP to operate on an extended schedule (including days or shifts not normally scheduled), curtailed basis, at a different level of service, or not at all. This includes changes in security condition levels for the facilities, which impact normal operations. The SP shall perform emergency support as required by the DGR on a task basis. The SP shall establish and maintain a notification system capable of notifying SP key personnel of critical system failures and security alarms during non-duty hours. The SP shall develop and submit to the DGR for approval the SP's Emergency Situations and Contingency Operations Support Plan within 30 days of Contract start date.

Extreme weather conditions (tornado, flooding, snow, and ice) may warrant temporary office evacuation or office closure. The SP shall respond to extreme weather conditions according to DGR direction, and shall inform all employees of these instructions. Announcements of facility closures will be made in the following manner: during normal duty hours, notification will be given through normal chain of management; during non-duty hours, notification will be made through local radio and television channels. Facility closings shall in no way interfere with the SP operation and/or maintenance of the critical systems. All SP employees identified as essential personnel shall remain on duty or report for duty in accordance with the Emergency Situations and Contingency Operations Support Plan.

The SP shall participate in all scheduled and unscheduled fire drills or other scheduled safety and emergency-training exercises, which may necessitate interrupted services unless directed otherwise. Such interruptions will be considered when assessing SP performance for the affected period. Drills and other scheduled training that requires the SP's support outside the normal duty hours of this PWS to support these events may be subject to an equitable adjustment for the affected period upon the SP providing sufficient documentation justifying the basis for the equitable adjustment. Interruptions or disruptions that result from participation or support of these events during normal working hours will not be considered a basis for an equitable adjustment.

5.6.7 Environmental Protection/Conservation of Utilities and Resources

The SP shall comply with all federal, state, and local environmental protection laws, regulations, and standards. The SP shall instruct SP employees in utilities conservation and recycling practices maintained within Government facilities. The SP shall comply with the various DOE facility installation energy conservation plans and participate in those energy conservation activities.

5.6.8 Safety and Occupational Health

All work shall be conducted in a safe manner and in compliance with but not limited to OSHA, EPA, and DOE requirements. Failure to comply with all applicable Federal, State, and Local laws and regulations

may result in a Stop Work Order for the affected work as issued by the CO. The SP shall maintain and report to the Government an accurate record of accidents and incidents resulting or causing injury or death and accidents resulting in damage to government property, supplies, and equipment.

5.6.9 Travel Requirements

Completion of the Task assignments described in this PWS will require the SP to travel within the Washington, D.C. metropolitan area and other field locations. The Government may or may not be required to reimburse the contractor for local travel, based on approval of the DGR. Some long distance travel may be required. Such travel must be approved in advance by the DGR; this will be set-up in the Task assignment as an ODC pool

SECTION 6: GOVERNMENT FURNISHED PROPERTY AND SERVICES

6.1 General

The Government will provide facilities, utilities, equipment, parts, supplies, and materials described in *TEs 6-1: Government Furnished Facilities, 6-2: Government Furnished Equipment,* and *3-6: SP Supported Software and Applications.* GFP for the purposes of this PWS consists of, Government Furnished Facilities (GFF), Government Furnished Equipment (GFE), Government Furnished Supplies and Material, and Government Furnished Utilities placed in the SP's custody. Property for which the SP shall be responsible for maintenance and support, but which remains in Government custody, is listed in *TE 3-6: SP Supported Equipment.* The Government will also provide certain services to the SP. The SP shall not use GFP or services for any other purpose than execution of work under this PWS.

6.1.1 Service Provider Accountability

The SP shall become accountable for GFP when the DGR transfers it from the Government accountable records to the SP, in compliance with normal DOE procedures. The SP shall meet property administration requirements contained in FAR Part 45 and applicable DOE regulations. The SP shall not remove GFP from DOE property or other supported areas without written approval from the DGR.

6.1.2 Inventory Management

The SP shall attend a phase-in GFP transfer and inventory meeting with the DGR. The Government will schedule the meeting prior to the Contract start date. Within ten (10) business days of the Contract start, the SP shall conduct phase-in joint inventory in accordance with DOE procedures in force at each affected DOE site. This inventory shall include, but is not limited to: GFF, GFE, and GFM. Activities to be inventoried will be designated by the DGR. This provision does not preclude prior inspection of GFP by the SP. The operational or conditional status of all GFF and GFE shall be determined. Any item found to be broken or not suitable for its intended purpose shall be recorded. The DGR and the SP shall certify the joint inventory as being accurate. The SP shall keep the inventory listing current in accordance with FAR Part 45.508 and applicable DOE regulations, orders, and directives.

6.1.3 Periodic Inventory

The SP shall establish and maintain records of GFP in use by the SP. The records shall be maintained in accordance with the functional guidance for the automated system in use or manually in accordance with the instructions contained in the FAR Part 45.508 and DOE regulations orders, and directives. The DGR shall review the records system and direct the SP to make appropriate changes to the record system established by the SP. Upon approval by the DGR, the records system shall become the SP's official GFP control system. It shall remain in use until termination of the Contract or written withdrawal of approval by the DGR.

The SP shall conduct an annual physical inventory of all non-expendable, durable GFP. The SP shall inventory accountable items in accordance with FAR Part 45. The SP shall also submit a report of the results of the physical inventory to the DGR within ten (10) business days of inventory completion. The SP shall conduct special inventories as requested by the DGR. The SP shall prepare recommended changes to the inventory and provide them to the DGR within 30 calendar days of inventory completion.

6.1.4 Phase-Out Inventory

The SP shall attend a phase-out GFP transfer and inventory meeting with the DGR. The Government will schedule the meeting approximately 60 calendar days prior to Contract completion or termination date.

One month prior to completion or termination of the Contract, an inventory of all GFP shall be conducted by the SP and observed by the Government in accordance with FAR Part 45.508. The Inventory shall include the same data as required for the initial inventory.

During the final inventory, all GFP shall be jointly inspected. All valid discrepancies shall be noted and may be corrected by one or both of the following methods at the Government's option. The SP shall correct noted discrepancies prior to Contract expiration, or, the cost of repair shall be deducted from the

final payment to the SP in accordance with instructions of the DGR. The DGR will determine the validity of the discrepancies.

At the completion of the Contract, the SP shall return the same property or property equal in type, kind, quality, and quantity of items as originally furnished by the Government and accepted by the SP less assets disposed of in accordance with the direction of the DGR. Government property shall be in the same or better condition as when originally furnished, less normal wear and tear.

6.1.5 Security

The SP shall be responsible for the physical security of GFP in the custody of the SP based on the requirements of this PWS. The SP shall secure all GFF when not occupied by SP personnel. The SP shall maintain an activity security checklist for each individual facility as part of the SP's Physical Security Program.

6.1.6 Change of Status for GFP

When GFP is no longer required or suitable for intended use, or has reached the end of its economic life, the SP shall prepare and provide a recommendation for disposition to the DGR for approval and disposition directions. Upon approval, the SP shall process the items in accordance with applicable Federal regulations (i.e., DOE guidance, General Services Administration (GSA) regulations and Federal Property Management Regulation (FPMR)). All property furnished under and all scrap resulting from this PWS shall remain the property of the Government.

6.2 Government Furnished Facilities

6.2.1 General

The Government will furnish or make available to the SP facilities listed in *TE 6-1: Government Furnished Facilities*. This list describes the Government Furnished (GF) office and storage space for the use of the SP's staff. Office space for administrative staff will include approximately 100 square feet of space per person. The SP shall not relocate activities or operational units within assigned facilities unless approved by the DGR.

The SP shall make no modifications to the GFF under this PWS without prior approval of the DGR. Damages to Government facilities that are determined to be the fault of the SP shall be repaired at no expense to the Government as directed by the DGR. The SP shall return facilities to the Government in the same condition as received, except for fair wear and tear and approved modifications.

The GFF will be in compliance with OSHA Standards. The SP is otherwise responsible for ensuring the assigned workplace and work practices comply with OSHA standards. If a latent hazard is later discovered, the Government will restore the area to acceptable OSHA standards at no cost to the SP. The SP is responsible for operating an occupational safety and health program to prevent accidents to SP employees, the public, and DOE personnel.

6.2.2 Final Condition

The Government reserves the right to reallocate and relocate assigned facilities during the term of the Contract. Upon completion or termination of this Contract, or during such reallocation/relocations, GFF shall be returned to the Government in the same condition as received, except for fair wear and tear and approved modifications in accordance with FAR 45.508.

6.2.3 Government Access

Authorized Government personnel shall have access to all GFF used by the SP. Government personnel may perform unscheduled visits during normal working hours. Access by other Government personnel shall be in accordance with facility procedures and policies and the Physical Security Plan (*Section 5.3.4* Physical Security Plan above).

6.3 Government Furnished Utilities

The SP shall have access to the utilities at the GFF locations. Types of utility services may include electricity, gas, water, sewage, steam, fuel oil, and liquid propane gas. All facilities do not receive the same utility services. The SP shall not change or modify any utility system or component without prior Government review and written approval.

6.4 Government Furnished Equipment

GFE is equipment provided to the SP for use in performing work specified in this PWS. The SP shall not use GFE for any other work unless prior authorization is received from the DGR. The Government will make available to the SP, on a one-time basis, in "as is" condition, GFE listed in TE *6-2: Government Furnished Equipment.* Any additional equipment deemed necessary by the SP outside of the GFE listings shall be procured at the expense of the SP, will remain property of the SP, and will not be charged directly to this Contract.

6.4.1 Accountability

The SP shall prepare the forms required for justification, deletions, and changes to GFE items authorized on the joint inventory in accordance with FAR PART 45. The SP shall furnish to the DGR, upon request, a listing of all non-expendable GFE in the format provided in the GFE listing attached to the Contract.

6.4.2 Transfer

The Government retains the right to withdraw any GFE at any time during the performance of the Contract. Additionally, all items of equipment will be deleted from GFE listing upon disposition in accordance with FAR PART 45. Any such disposition of GFE will be accomplished in accordance with the Contract General Provision entitled "Government Property". If replacement equipment is required to perform work required in this PWS, the SP shall submit a proposal to the DGR for approval for replacement of the disposed equipment.

6.4.3 Replacement

The SP shall submit to the DGR written documentation for justifying new or replacement equipment purchases for which the DGR has indicated Government responsibility. Upon approval of the DGR, the SP is authorized to purchase the equipment for the Government under this PWS. If replacement is required due to SP negligence or misuse, the SP shall reimburse the Government for the full replacement cost. Equipment purchased by the SP at Government expense for the Government shall be added to the SP's property control inventory and returned to Government control after completion of the Contract.

6.5 Government Furnished Services

6.5.1 Emergency Services

The SP shall have access to the Government emergency services available at GFF locations.

In the event an SP employee suffers a serious or life-threatening injury, emergency treatment will be provided as the first point of medical care. Transfer to other than Government medical treatment facilities shall be accomplished as soon as possible and as determined by attending medical authorities.

The Government will provide fire prevention, fire protection and inspection of GFP, and maintenance of GF fire extinguishers and systems. The SP shall cooperate with all fire programs, drills and instructions.

Where applicable, the Government will provide the security protection of the local federal security contract to the SP while on Government property. The SP shall cooperate with all security programs, drills and instructions.

6.5.2 Communications

The SP shall have access to the Government communication services available at GFF locations.

SP personnel shall not relocate GF telephone communications equipment, nor change in any way the telephone distribution system except at the direction of the DGR. Whenever changes to communication

services are required, to include changing locations of extensions and adding and deleting phone lines, the SP shall prepare and submit a request to the DGR. The SP shall obtain Government approval before connecting or disconnecting any Service Provider Furnished Equipment (SPFE) to GF communications systems, lines, or equipment.

The SP shall not utilize the GF communication services for any action not directly associated with the requirements of this PWS.

Video-teleconference facilities in operation on DOE sites will be available for SP use according to local policies in performance of official functions as required by this PWS.

The Government will provide telephone service for official use only through the Government system for on-site, local area and long distance calls for purposes of performance of the work identified in this document.

6.5.3 Mail and Other Correspondence

The SP shall have access to the internal and external Government mail services available at GFF locations. The SP shall return all misdirected mail to the central location. The Government will pay all postage, shipping, and handling fees generated by the SP in providing official Government services required by this PWS. The SP shall be responsible for all other postage, shipping, and handling fees.

6.5.4 Trash Removal

The SP shall have access to the Government trash removal services available at GFF locations.

SECTION 7: SERVICE PROVIDER FURNISHED PROPERTY (SPFP) AND SERVICES

7.1 General

7.1.1 Provision, Storage, and Removal

The SP shall furnish all property not specifically identified as GF in *TE 6-2: Government Furnished Equipment* necessary to comply with the requirements of this PWS. Property may include, but is not limited to, IT equipment, systems, applications, supplies, repair parts, ID system camera and badges, and timekeeping system. The SP shall ensure that the SP's systems are compatible with DOE systems and architecture unless otherwise directed by the DGR.

7.1.2 Separation or Commingling of Property

Government property shall be kept physically separate from SP-owned property to the maximum extent practicable at the direction of the DGR. When advantageous to the Government and consistent with the SP's authority to use such property, and with the approval of the DGR, the property may be mixed. Within 30 calendar days after completion or termination of this PWS, the SP shall remove all SP-owned equipment, tools, supplies, materials and other items from the facility locations. The Government shall not be responsible for any SP-owned property left after Contract completion or termination.

7.2 Facilities and Utilities

The SP may request additional GFF upon determining a need for them. The SP shall include specifications and justification for the needed facilities in the request to the DGR. If the request is approved, the DGR will determine the availability of suitable facilities. If no facilities are found, the SP may submit proposed locations and associated costs. Facilities and utilities required by the SP to supplement those provided as GF will be obtained at the SP's expense, except as authorized by the DGR

7.3 Equipment and Supplies

The SP shall furnish all equipment and material, including Automated Data Processing Equipment (ADPE), and administrative equipment, not furnished by the Government but required for performance of work required under this PWS. Equipment condition shall not relieve the SP of any responsibility to provide services as required in this PWS. Tools and equipment acquired by the SP at SP cost to supplement those provided as GF shall remain the property of the SP upon termination or completion of the Contract, except as otherwise directed by the DGR.

7.3.1 Compliance with Requirements

All SP-furnished materials, supplies, parts, etc. shall meet manufacturer specifications or Government approved deviations. The SP-furnished equipment shall meet the same safety requirements as those established for Government equipment.

7.4 Services Provided by the Service Provider

7.4.1 Communication Services

The SP shall obtain those communication services required to perform work specified in this PWS that are not GF to include, but not limited to, cellular telephones, pagers, and PDAs. SP communication services will be subject to standard monitoring requirements of the Government telephone network. Exceptions may be authorized by the DGR.

SECTION 8: TRANSITION CONTINUITY OF OPERATIONS

8.1 Transition Period

In order to ensure the smooth transition to SP performance and to prevent possible decreases in productivity or service quality, the Government will provide, at a minimum, a 60 Calendar-day transition period following the final decision date. The transition period coincides with the contract start date and precedes the assumption of full SP responsibility. During this transition period, the Government will make available to key SP personnel, a DGR familiar with the operations, processes, and functions to be performed. The Government will make all facilities and equipment accessible to the SP for a maximum of 60 days prior to the Contract start date. During the first 30 days of this period, the SP's personnel will be permitted to observe any Information Technology operations at DOE facilities. This service is being made available, if applicable, to explain procedures for conducting Government business, show the SP the worksites, and introduce the SP to customer representatives.

During the transition period, the SP shall organize, plan, recruit personnel, train, mobilize, develop procedures, and accomplish all actions necessary to commence performance of the services at the end of the transition period. The Government will provide the CO with a list of adversely affected employees as required by OMB Circular A-76 and FAR 7.305(c) regarding the Right of First Refusal in the event of a private sector performance decision.

During the transition period, the SP shall:

- Establish the Project Management Office
- Recruit and hire necessary personnel
- Obtain all required certifications
- Obtain required clearances, including personnel security clearances (this process generally takes 6 to 18 months)
- Participate in joint inventories and sign for GFP
- Develop and submit any required deliverables
- Attend post-award meetings as required
- Accomplish any necessary training to support the Performance Objectives and Measures listed in *Section 3: Performance Objectives and Measure*
- Create SOPs for each functional area covered under this PWS unless otherwise provided by the Government. Content could include: QC, hours of operation, work assignments, approval authorities, work flow, functional relationships between the Government and the SP and between the SP's organizational elements, and any other information needed for efficient and uniform performance.

8.1.1 Transition Plan

The SP shall submit a Transition Plan with its proposal that addresses all the aforementioned areas in sufficient detail for the Government to determine if the plan satisfactorily meets the requirements of this PWS. The Transition Plan is a written plan that supports the orderly and progressive transition from full performance under the pre-award organizational structure to full performance by the SP. It shall be designed to minimize the disruption and adverse impacts, and describes capitalization and start-up requirements. The Transition Plan shall address transition costs such as proposed process improvements, if applicable, mobilization, training, observing performance, staffing, and development and dissemination of the operational procedures. The Transition Plan shall also include a listing of milestones that chronicle the SP's sequence of transition period events and address both phase-in and phase-out activities. No less than 10 calendar days prior to transition period start date, the SP shall provide an updated Transition Plan and milestones. There will be no interruption to mission requirements as defined in the PWS.

8.1.2 Phase-In Period

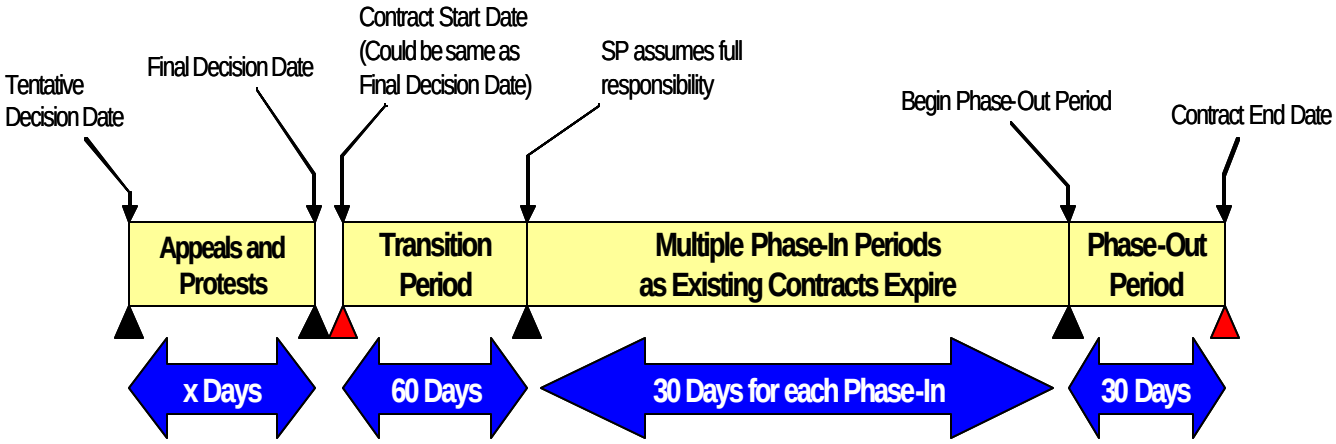
For all work of this PWS that continues to be performed by existing contracts after this contract start date, there may be a 30-day phase in period for each expiring contract, during which the SP shall assume full responsibility for continuation of performance. This will be task specific as directed by the DGR. During the phase-in period(s) the SP shall take all actions necessary for a smooth transition of all Information Technology operations.

8.1.3 Phase-Out Period

The current SP shall develop and submit a comprehensive phase-out plan sixty (60) calendar days prior to completion of the base period, or termination, of the resulting contract. The SP's phase-out plan shall not disrupt or adversely impact the day-to-day conduct of Government business and shall achieve a smooth and orderly transfer of responsibility to a successor.

Thirty (30) calendar days prior to the completion of this PWS, an observation period shall occur, at which time, personnel of the incoming workforce may observe operations and performance methods of the outgoing SP. This will allow for orderly turnover of facilities, equipment, and records and will help to ensure continuity of service. The outgoing SP shall not defer any requirements for the purpose of avoiding responsibility or of transferring such responsibility to the succeeding SP. The outgoing SP shall fully cooperate with the succeeding SP and the Government so as not to interfere with their work or duties.

Below is a diagram, depicting the timeline for the Transition Continuity of Operations:



SECTION 9: QUALITY CONTROL AND QUALITY ASSURANCE

9.1 Quality Control

The SP shall submit a proposed Quality Control Plan (QCP) that contains the items listed below, as part of the SP's overall technical proposal. The SP shall make appropriate modifications to the plan as directed by the DGR. An updated QCP shall be provided to the DGR at least ten (10) business days prior to implementation of any changes that are required during the performance of this PWS.

The QCP shall:

- Establish an assessment plan covering all services required by this PWS specifying areas to be reviewed on both a scheduled or unscheduled basis, and the title of the individual who will perform the assessment.
- Describe a method acceptable to the Government for identifying, preventing, and resolving deficiencies in the quality of service performed under this PWS before the level of performance becomes unacceptable and that also addresses processes for corrective actions without dependence upon Government direction.
- Include a customer complaint feedback system/survey/questionnaire for correction of validated complaints and to inform the customer of corrections.
- Describe methods of direct and indirect communications with the DGR regarding performance of the PWS, to include regular and formal meetings with the DGR.

Assessment records and associated documentation shall be made available to the Government throughout the Contract performance period or as directed by the DGR.

9.2 Quality Assurance

The DGR will provide Quality Assurance (QA) by evaluating the SP's performance under this PWS. The DGR will evaluate the SP's overall performance and compliance with the PWS on the basis of those factors that are under the SP's control. Such factors may include, but are not limited to: compliance to the SP QCP, compliance to the PRS, compliance to plan of operation, compliance to internal work specifications and timeliness, customer satisfaction, safety practices, emergency response and responsiveness, and quality of performance.

For those services listed in *Section 3: Performance Objectives and Measures*, the Quality Assurance Evaluator(s) (QAE(s)) will follow the methods of surveillance specified in the Federally prepared Quality Assurance Surveillance Plan (QASP) for this Contract and record all surveillance observations. When an observation indicates deficient performance, the QAE will notify the COR immediately as well as require the SP Project Manager (PM) or designated representative at the site to initial the observation. Initialing of the observation does not constitute concurrence that performance is deficient; rather it acknowledges that the PM has been made aware of the QAE's observation. Upon acknowledgement, the SP shall evaluate the observation and take appropriate action as necessary. The DGR may increase the number of inspections because of repeated failures discovered during periodic inspections or because of repeated customer complaints. Likewise, the DGR may decrease the number of QC inspections if performance dictates.

The SP shall meet with the COR at least once weekly during the first two (2) months of the Contract. Thereafter, the DGR will schedule meetings as necessary, but not less than once during each quarter of the performance period under this PWS.

APPENDIX A: DEFINITIONS AND ACRONYMS

A.1 Definitions

Acceptable Quantity Level (AQL) - Represents the required success rate for each output that comprises the total workload. The AQL is reasonable to allow for the possibility of unexpected problems that prevent some outputs from meeting the requirements of the performance standards. The AQL is a percentage value of the number of performances of each output that must adhere to the performance standard set for that output. AQLs are determined based on agency directives or historical records of Government performance.

Accountability: Accountability is the obligation of both the SP and the Government to fulfill the requirements of this contract. This includes, but is not limited, the SP's responsibility to maintain accurate and complete records of property, documents, or funds.

Accreditation: The formal declaration by a Designated Approving Authority (DAA) that an IS is approved to operate in a particular security mode using a prescribed set of safeguards to an acceptable level of risk.

Automated Information System (AIS) - Computer hardware, computer software, telecommunications, IT, personnel, and other resources that collect, record, process, store, communicate, retrieve, and display information. Can include computer software only, computer hardware only, or a combination of the above.

Availability: A measure of the degree to which an item is in an operable and committable state at the start of any task or mission, when the task or mission is called for at an unknown (random) point in time.

Baseline - A specification or product that has been formally reviewed and agreed upon, and thereafter serves as the basis for further development and can be changed only through formal change-control procedures or a type of procedure such as configuration management (CM).

Biennially: One time every two years.

Bimonthly: One time every two months.

Biweekly: One time every two weeks.

Cancellation: A total or partial discontinuance of tasks specified and confirmed by the authorized DGR.

Certification: Certification is the comprehensive evaluation of the technical and non-technical security features of an Information System (IS) and other safeguards, made in support of the accreditation process, to establish the extent to which a particular design and implementation meets a set of specified security requirements.

Classified: Documents, data, information, systems, products, services, items, etc for which access is limited to those persons having a "need to know" and appropriate security clearance.

Clearance: Authority permitting individuals cooperating in DOE work, and having a legitimate interest therein, access to classified technical information, material, or equipment or admission to restricted areas or facilities where such information or material is located.

Commercial Off The Shelf (COTS): Describes software or hardware products that are ready-made and available for sale to the general public.

Common Operating Environment (COE) - A listing of components (hardware and software) that captures the concept of a common or shared operating environment across an enterprise or organization. Provides a standard for the organization to be common operating environment (COE) compliant.

Configuration Management (CM) - A discipline applying technical and administrative direction and surveillance to: (a) identify and document the functional and physical characteristics of a particular item,

system, etc; (b) control changes of those characteristics; and (c) record and report changes to processing and implementation status.

Configuration: The functional or physical characteristics of equipment, systems, hardware or software set forth in technical documentation and achieved in a product.

Conservation: The protection, improvement, and use of natural resources according to principles that will provide optimum public benefit and support of DOE's mission.

Contract Administrator: An individual duly assigned by appropriate authority to administer a contract.

Contract Modification: Any written alteration in the specifications, delivery point, rate of delivery, contract period, price, quantity, or other contract provisions of an existing contract by the Contracting Officer.

Contract Start Date: Effective date of the contract and beginning of the Transition Period as authorized by the CO at or following contract award.

Contract: All types of agreements and orders for the procurement of supplies or services.

Contracting Officer (CO): An individual appointed in accordance with procedures prescribed by the Federal Acquisition Regulation with the authority to enter into and administer contracts and make determinations and findings with respect thereto, or with any part of such authority.

Contracting Officer's Representative (COR): Any person who has been appointed in writing as the authorized representative of the Contracting Officer acting within the limits of his or her authority.

Controlled Inventory Items: Items with characteristics requiring special ID, accounting, security, or handling to ensure their safeguard.

Corrective Action: Consists of those efforts required to correct reported deficiencies and mitigate reoccurrence of defects.

Customer: Any recipient to a service described in Section 3: Performance Objectives and Measures of this contract.

Damage: A condition that impairs either value or utility of an article; may occur in varying degrees. Property may be damaged in appearance or in expected useful life without rendering it unserviceable or less useful. Damage also shows partial non-serviceability. Usually implies that damage is the result of some act or omission.

Designated Government Representative (DGR): The person(s) designated by name and/or position to act as a liaison between the Government and the Service Provider on all issues pertinent to the daily operation of the contract. The DGR is generally appointed by the CO or COR.

Discrepancy: A variance between contractually required and actual performance.

Disposal: The disposition of excess assets (including real property, industrial and personal property) by the government.

E-Gov: A PMA initiative, using technology to its fullest to provide services and information that is centered around citizen groups.

Emergency: The reporting of sudden, usually unforeseen, occurrences where life or property are in immediate danger and require immediate action.

Enterprise Architecture (EA): A description including graphics of the systems and interconnections providing for or supporting various functions. EA defines the physical connection, location, and identification of such key nodes as circuit and network platforms, and allocates system and component performance parameters. Is constructed to satisfy Operation Architecture requirements in the standards

defined in the technical architecture. Shows how multiple systems within a domain or an operational scenario link and interoperate, and may describe the internal construction or operations of particular systems in the systems architecture.

Facilities: Buildings or structures, in whole or in part, furnished by the Government or SP for contract performance.

Final Decision Date: The point at which performance decision/source selection decision is definitive.

Fiscal Year (FY): A period of 12 months beginning 1 October and ending 30 September of the following year. Fiscal year is designated by the calendar year in which it ends.

Government Furnished Equipment (GFE): A term used in this contract to mean equipment in the possession of, or directly acquired by, the Government and subsequently made available for the sole use of the SP in the performance of this contract.

Government Furnished Property (GFP): A term used in this contract to mean property in the possession of, or directly acquired by, the Government and subsequently made available for the sole use of the SP in the performance of this contract.

Government Off The Shelf (GOTS): Software developed for and owned by the government.

Graphical User Interface (GUI) - The use of pictures rather than just words to represent the input/output (I/O) of a program. A program with a GUI runs under some windowing system [for example, X Window System, Microsoft (MS) Windows, Acorn Reduced Instruction Set Computer (RISC) operating system (OS), NEXTSTEP]. The program displays certain icons, buttons, and dialogue boxes in its windows on the screen. The user controls the icons mainly by moving a pointer on the screen, typically controlled by a mouse, and selecting certain objects by pressing buttons on the mouse while the pointer is pointing at them.

Guidance: A statement of direction including, but not limited to, rules, laws, regulations, guidelines, and directives.

I-Manage: TBD

Information Technology Management (ITM): Activities related to management support of IT related policy development, strategic planning, capital planning, resource management, and special projects.

Infrastructure: Identifies the top-level design of communications, processing, and OS software and describes the performance characteristics needed to meet database and application requirements. It includes processors, Operating Systems, service software, and standards profiles that include network diagrams showing communication links with bandwidth, processor locations, and capacities to include hardware builds versus schedule and costs.

Inspection: Determination and identification of the condition of equipment, facilities, and systems with reference to contractual requirements.

Integration: The result of an effort that seamlessly joins two or more similar products (for example, individual system elements, components, modules, processes, databases, or other entities) to produce a new product. The new product functions as a replacement for two or more similar entities or products within a framework or architecture.

Integrator: A public or private sector entity that develops, assembles and executes a comprehensive solution to complex information technology requirements.

Interoperability: The condition achieved when information can be exchanged directly and satisfactorily between two or more systems or components

Intrusion Detection System: Provides an additional layer of assurance through the monitoring of network activity to detect and report suspicious, unauthorized, or harmful activities.

Inventory Control: The process of managing, cataloging, and accounting for property provided under this contract.

Joint Inventory: A physical count of assets conducted by the SP and the Government for the purpose of establishing the quantity and condition of property accountable to the contract.

Knowledge Management: The systematic process of finding, selecting, securing, organizing, distilling, and presenting information in a way that maintains an ongoing DOE corporate knowledge, that is input to and/or resulting from, the execution of the performance requirements under this PWS.

Lot Size: Number of units or product of output from which a sample is derived.

Maintenance: The support and repair of information technology hardware and software in accordance with applicable specifications, including but not limited to diagnosing failures, performing corrective action to ensure proper operation.

Normal Wear and Tear: Loss or impairment of appearance, effectiveness, worth, or utility of an item that has occurred solely because of normal and customary use of the item for its intended purpose.

On-Site Assistance: A visit to an activity in response to a request by the activity for assistance in resolving a records management issue within the activity. A follow-up memorandum will summarize the issue and recommendation.

On-Site: Repairs or services performed at a customer's location.

Organization: An administrative structure with a mission. The term is used in a very broad sense throughout this document.

Performance Requirements Summary (PRS): The portion of the PWS which documents contract requirements, the component requirements related to each contract requirement, and the standards and measures of performance.

Performance Standard: A selected characteristic of an output of a work process that can be measured, indicating acceptable performance.

Performance Work Statement (PWS): portion of the contract that identifies the requirements and objectives.

Phase-in Period: The period(s) during which the SP deals with the transfer of performance responsibility from existing contractors to the SP.

Phase-out Period: The 30-day period prior to completion of the contract. See Section *8.1.3: Phase-out Period* for further detail.

Planned Sampling: Based on some subjective rationale and sample size arbitrarily determined.

Preventive Maintenance: Systematic and cyclic check, inspection, servicing, and repairs of deficiencies, as well as reporting of deficiencies beyond scope of PM. PM includes accomplishment of maintenance and repair.

Program: An organized set of activities directed toward a common purpose, objective, or goal undertaken or proposed by an Agency to carry out assigned responsibilities. The term is generic and may be applied to many types of activities. Acquisition programs are programs whose purpose is to deliver a capability in response to a specific mission need. Acquisition programs may comprise multiple acquisition projects and other activities necessary to meet the mission need.

Project: A single undertaking or task involving maintenance, repair, construction, or equipment-in-place, in which a facility or group of similar facilities are treated as an entity with a finite scope.

Property: Terms "Real Property", "Government Property", "DOE Property", and "Property" include all property under control of DOE or the SP on behalf of DOE. Property includes but is not limited to land, facilities, equipment, supplies, parts, and accessories thereto, and alteration or Facility of any of the foregoing.

Quality Assurance (QA): Actions taken by the Government to inspect or check goods and services to determine that they meet or do not meet requirements of the contract. See QASP for further detail.

Quality Assurance Evaluator (QAE): That person responsible for surveying the SP performance.

Quality Assurance Surveillance Plan (QASP): An organized written document used by Government for quality assurance surveillance. Document contains sampling/evaluation guides, checklists, and the Performance Requirements Summary (PRS).

Quality Control (QC): Those actions taken by a Service Provider to control the performance of services so they meet the requirements of the PWS. See Quality Control Plan for further detail.

Quality Control (QC) Plan: SP's system to control the equipment, systems, or services so that they meet the requirements of the contract.

Random Sample: A sampling method whereby each service output in a lot has an equal chance of being selected.

Reportable Incident – Any event, suspected event, or vulnerability that could pose a threat to the integrity, availability, or confidentiality of systems, applications or data. Incidents may result in the possession of unauthorized knowledge, the wrongful disclosure of information, the unauthorized alteration or destruction of data or systems and violation of federal or state laws. If such violations are detected or suspected, they are to be reported immediately to a security manager.

Requirement - A need or demand. A subtype of guidance. May be specified in other guidance or derived from necessity and circumstances. Effort mandated by this PWS and as directed by the COR within the scope of the resulting contract.

Restricted Area: Those areas designated by DOE that require control of personnel for security reasons and/or equipment for protection of personnel, property and information.

Routine Call: A request for service with a response time as defined in the Technical Exhibits.

Sample: A sample consists of one or more service outputs drawn from a lot, the outputs being chosen at random.

Sensitive: Documents, data, information, systems, products, services, items, etc requiring protection and control because of statutory requirements or regulations.

Service Call: Any notification or request for service as defined in the Technical Exhibits.

Service Provider: The Government or private sector organization that will serve as an integrator to develop, assemble and execute a comprehensive solution to complex information technology requirements contained in this PWS and resulting contract.

Service Provider-Furnished Equipment (SPFE): That equipment that the SP includes in its offer in order to perform the requirements of the contract, and that is not covered under GFP. The SP retains title to all SPFE.

Service Provider-Furnished Property (SPFP): That property that the SP includes in its offer in order to perform the requirements of the contract, and that is not covered under GFP. The SP retains title to all SPFP.

Shall: The word "Shall" is used in connection with the SP and specifies that the provisions are mandatory.

Site Offices/Locations : Those support locations, offices, and facilities listed in TE-2-1.

Standard Operating Procedure (SOP): A comprehensive narrative description of maintenance and repair methods prepared by the SP or provided by the government. A set of instructions covering those features of operations that lend themselves to a definite or standardized procedure without loss of effectiveness. The procedure is applicable unless ordered otherwise.

Supplies: Items needed to equip, maintain, operate, and support the requirements of this PWS and the resulting contract

System: Any entity that has input, process, output and feedback.

Task: An activity with associated resources that is directed by the COR or DGR in accordance with the PWS and the resulting contract.

Transition Period: A 60-day period following contract start date, during which the SP will prepare to assume full responsibility for performance of the contract. During this period, the SP shall organize, plan, recruit personnel, train, mobilize, develop procedures, and accomplish all actions necessary to commence performance of the services at the end of the transition period.

User: A person, organization, or other entity that employs IT related services provided under this PWS and the resulting contract.

Utilities: Electricity, gas, water, sewage disposal, and steam are types of utilities used under the performance of this PWS and the resulting contract.

Vulnerability Assessment/Analysis: Identifying, characterizing, and testing potential security exposures.

Workstation: A terminal, desktop, or laptop computer in a network. In this context, workstation is a generic term for a user's machine (client machine).

A.2 Acronyms

ADPE	Automated Data Processing Equipment
AQL	Acceptable Quality Level
BAO	Building Access Only
CA	Commercial Activities
CCB	Change Control Board
CCP	Configuration Change Proposals
CIAC	Computer Incident Advisory Capability
CIO	Chief Information Officer
CFR	Code of Federal Regulations
CM	Configuration Management
CMM	Capability Maturity Model
CO	Contracting Officer
COB	Close of Business
COE	Common Operating Environment
COOP	Continuity of Operations Plan
COR	Contracting Officer's Representative
COTS	Commercial off the Shelf
CRM	Customer Relationship Management
CSPP	Cyber Security Program Plan
DAA	Designated Approval Authority
DGR	Designated Government Representative
DOD	U.S. Department of Defense
DOE	U.S. Department of Energy
EA	Enterprise Architecture
ED	Office of Economic Impact and Diversity
EE	Office of Energy Efficiency and Renewable Energy
EH	Office of Environment, Safety and Health
EIA	Energy Information Administration
EM	Office of Environmental Management
EPA	Environmental Protection Agency
ERP	Enterprise Resource Planning
FAQ	Frequently Asked Questions
FAR	Federal Acquisition Regulation

FAIR	Federal Activities Inventory Reform Act
FE	Office of Fossil Energy
FEA	Federal Enterprise Architecture
FPMR	Federal Property Management Regulation
FY	Fiscal Year
GAO	General Accounting Office
GC	General Counsel
GF	Government Furnished
GFE	Government Furnished Equipment
GFF	Government Furnished Facilities
GFP	Government Furnished Property
GOTS	Government off the Shelf
GPEA	Government Paper Elimination Act
GPRA	Government Performance and Results Act
GSA	General Services Administration
HG	Office of Hearings and Appeals
IAW	In accordance with
ID	Identification
IG	Office of Inspector General
IGE	Independent Government Estimate
IM	Information Management
IN	Intelligence Office
ISDN	Integrated Services Digital Network
ISO	International Standards Organization
IT	Information Technology
ITM	Information Technology Management
ITMRA	Information Technology Management Reform Act of 1996 (a.k.a. Clinger-Cohen Act)
JFMIP	Joint Financial Management Improvement Program
KM	Knowledge Management
LAN	Local Area Network
ME	Office of Management, Budget, and Evaluation
NARA	National Archives and Records Administration
NE	Office of Nuclear Energy, Science, and Technology
NETL	National Energy Technology Laboratory
NIST	National Institute of Standards and Technology

NNSA	National Nuclear Security Administration
O	Order
OA	Office of Independent Oversight & Performance Assurance
OCIO	Office of the Chief Information Officer
ODC	Other Direct Costs
OMB	Office of Management and Budget
OSHA	Occupational Safety and Health Administration
P	Publication
PCSP	Program Cyber Security Plan
PDA	Personal Digital Assistant
PDD	Presidential Decision Directive
PI	Office of Policy & International Affairs
PM	Project/Program Manager
PMA	President's Management Agenda
POC	Point of Contact
PRS	Performance Requirements Summary
PWS	Performance Work Statement
QA	Quality Assurance
QAE	Quality Assurance Evaluator
QASP	Quality Assurance Surveillance Plan
QC	Quality Control
QCP	Quality Control Plan
RW	Office of Civilian Radioactive Waste Management
SC	Office of Science
SEI	Software Engineering Institute
SO	Office of Security
SOP	Standard Operating Procedure
SP	Service Provider
SPFE	Service Provider Furnished Equipment
SPFP	Service Provider Furnished Property
STD	Standard
TA	Task Assignment
TE	Technical Exhibit
USC	United States Code
WAN	Wide Area Network

WT Office of Worker and Community Transition

APPENDIX B: TECHNICAL LIBRARY

B.1 Applicable Directives

The Contractor shall fully comply with all current applicable laws, regulations, DOE procedures, and DOE Directives (active series) which are, in part, identified below. Additional specific directives will be identified in each task order. The DOE directives are available at http://www.explorer.doe.gov.

- DOE M 200.1-1 Telecommunications Security Manual
- DOE M 471.2-1B Classified Matter Protection and Control Manual
- DOE M 475.1-1 Identifying Classified Information
- DOE N 142.1 Unclassified Foreign Visits and Assignments
- DOE N 203.1 Software Quality Assurance
- DOE N 205.1 Unclassified Cyber Security Program
- DOE N 205.3 Password Generation, Protection, and Use
- DOE N 206.1 Electronic Mail Analysis Capability
- DOE N 430.2 Extension of In-house Energy Management
- DOE N 471.2 Extension of DOE Order 471.2A
- DOE N 473.4 Department of Energy Badges
- DOE O 231.1, Chg. 2 Environment, Safety, and Health Reporting
- DOE O 200.1 Information Management Program
- DOE O 414.1A Quality Assurance
- DOE O 420.1 Facility Safety
- DOE O 430.2 In-house Energy Management
- DOE O 451.1A National Environmental Policy Act Compliance Program
- DOE O 470.1 Safeguards and Security Program
- DOE O 471.2A Information Security Program
- DOE P 142.1 Unclassified Foreign Visits and Assignments
- DOE P 450.4 Safety Management System Policy
- DOE P 450.6 Secretarial Policy Statement, Environment, Safety, and Health
- DOE 2030 Reporting Fraud, Waste, and Abuse to the Office of Inspector General
- DOE 4300.1C Real Property Management
- DOE 4320.2A Capital Management Asset Process
- DOE 5480.4 Environmental Protection, Safety, and Health Protection Standards
- DOE 5610.2 Control of Weapon Data

B.2 Links to Other Applicable Guidance

- Cyber Security Program Plan (CSPP) Template and Guidance dated November 5, 1999. Comments or questions may be directed to: The Office of Cyber Security (202)-586-1077.
- Cyber Security Architecture Guidelines - final version, dated May 2000
- Use of Warning Banners on Departmental Computer Systems> signed by John M. Gilligan, dated June 17, 1999
- Six Further Enhancements to DOE Cyber Security, dated May 1999
- Appropriate Use of the Internet, dated February 1996
- Time, dated June 1996
- CIO Council Review and Approval of Limited Personal Use Policy, dated March 1999

- DOE Guidance for Preparation of Acceptable Use Agreements for Users of Computational Resources, dated December 1995, Revised June 1998
- DOE Guidance for Providing Information to the Public via Public Access Servers, dated November 1995, Revised June 1998
- Information Management Strategic Plan (WordPerfect) (PDF)
- Executive Order 13130 of July 14, 1999 - National Infrastructure Assurance Council
- Executive Order 13103 of September 30, 1998 - Computer Software Piracy
- Executive Order 13111 of January 12, 1999 - Using Technology to Improve Training Opportunities for Federal Government Employees
- Executive Order 13011 of July 16, 1996 - Federal Information Technology
- Presidential Decision Directive 63 (PDD-63) - Protecting America's Critical Infrastructures- *dated May 1998*
- Executive Order 13010 of July 15, 1996 - Critical Information Protection
- Executive Order 13064 of October 14, 1997 - Amendment to Executive Order 13010, Critical Information Protection
- Executive Order Search - from the Whitehouse Web Page
- PKI - NIST Public Key Infrastructure Program
- E-FOIA/FOIA
- Clinger-Cohen Act
- SEC. 508. Electronic and Information Technology
- Architectural and Transportation Barriers Compliance Board (Access Board)
- Interpretation of the Electronic and Information Technology Accessibility Standards
- Federal Acquisition Regulation, Electronic and Information Technology Accessibility
- Federal Information Technology Accessibility Initiative (FITAI)
- World Wide Web Consortium (W3C)Accessibility Initiative
- Web Content Accessibility Guidelines 1.0
- Checklist of Checkpoints for Web Content Accessibility Guidelines 1.0
- Curriculum on Web Content Accessibility Guidelines
- Bobby

ATTACHMENT 1: TASK/SUBTASK TEMPLATE

ATTACHMENT 2: DGR TASK MONITOR HANDBOOK

ATTACHMENT 3: PERFORMANCE WORK STATEMENT COMMENT FORM