C.1 Performance Work Statement

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. All functions and activities will be task driven, and all work performed must be in accordance with all applicable regulations and guidelines as set forth in *Appendix B: Technical Library* or as instructed by the Contracting Officer's Representative (COR).

For purposes of this document, the term "Service Provider (SP)" refers to either the Government or private sector organization that will serve as the integrator to develop, assemble, and execute a comprehensive solution to the complex IT requirements outlined in this PWS. 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 PWS includes the workload and efforts of both Federal employees and IT support contractors currently performing the respective requirements across multiple locations. For the purpose of this solicitation, Offerors should bid to the entire workload included in *Technical Exhibit (TE) 3-1: Historical Workload Estimates*. The SP will not assume full responsibility for all workload upon Contract award. The SP will assume responsibility of requirements currently performed by other IT support contractors on a phased-in basis, to be determined at the task order level by the COR.

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 PMA 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 private sector 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 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 private sector contractor employees at complexes that consist 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

1.2.4 Concept of Operations

The Concept of Operations (ConOps) for DOE is a single integrated IT infrastructure for the Department. This ConOps is an opportunity to reduce DOE's operational costs and increase security. This model is common practice in both private industry and in agencies across the federal government. In this context, the DOE infrastructure generally incorporates utility-like functions that are similar across all components. Standardizing and consolidating like functions to achieve efficiencies is at the core of both OMB and DOE-sponsored e-Government initiatives. The scope of this PWS addresses the full range of services that support a single integrated infrastructure. The study does not address corporate business systems like I-MANAGE or mission specific systems that ride over the infrastructure. Management of corporate business and mission-specific systems will remain with the Program Offices.

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 TEs and Appendices as follows:

1. Introduction
2. Scope of Work
   - TE 2-1: Mission Statements by Organization
   - TE 2-2: Users by Program/Staff Office
   - TE 2-3: Users by Physical Location
3. Performance Objectives and Measures
   - TE 3-1: Historical Workload Estimates
   - TE 3-2: Performance Requirements Summary
   - TE 3-3: IT Infrastructure
   - TE 3-4: SP Supported Equipment
   - TE 3-5: SP Supported Software and Applications
   - TE 5-1: Security Clearance Requirementss
   - TE 6-1: Government Furnished Facilities
   - TE 6-2: Government Furnished Equipment

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. Technical Exhibits 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 enhance readability, TEs are referenced by italics, followed by a colon, and the name of the TE (e.g., *TE 3-1:Historical Workload Estimates*).

2. Scope of Work

2.1 Work Description

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

- **Information Technology Management** – Activities related to management support of IT related policy development, strategic planning, enterprise architecture, capital planning and investment control, resource management, procurement actions, and special projects

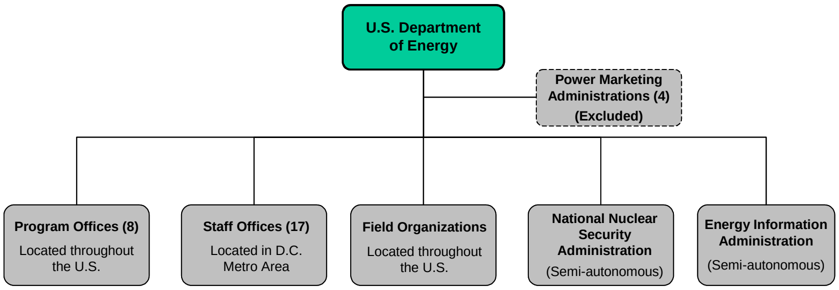
- **Systems Development and Engineering** – Activities pertaining to software development support for all existing, planned, and future DOE IT systems. Typical duties include capturing user and business owner requirements; coordinating with appropriate Departmental personnel regarding enterprise architecture; 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 includes network access and security; server management; emergency preparedness planning; IT disaster recovery planning and execution; IT inventory control; audio, video, and web conferencing; application system administration; user support; workstation management; IT training and education; wireless services; and voice and data services

- **Cyber Security** - Activities related to the secure transmission and storage of electronic information, drafting cyber security policy and procedures, providing user awareness training, risk management, and 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, one (1) semi-autonomous Agency, one (1) semi-autonomous Program Office and four (4) Power Marketing Administrations. Field Organizations located throughout the United States execute DOE's specific mission tasks. Seventeen (17) Staff Offices provide support to the Program Offices. The following diagram provides a high-level depiction of DOE's organizational structure. Detailed mission statements for each Program Office, Staff Office, and Field Organization and the semi-autonomous Agency are provided in *TE 2-1: Mission Statements by Organization*.


U.S. Department of Energy
Power Marketing Administrations (4) (Excluded)
Program Offices (8)
Located throughout the U.S.
Staff Offices (17)
Located in D.C. Metro Area
Field Organizations
Located throughout the U.S.
National Nuclear Security Administration
(Semi-autonomous)
Energy Information Administration
(Semi-autonomous)

2.2.1 Program Offices

A Program Office is responsible for executing program management functions, and for assisting and supporting Field Organizations in safety and health, administrative, management, and technical areas. The Program Offices also identify, develop, and direct various policies and programs to accomplish DOE'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: Mission Statements by Organization* and *TE 2-2: Users by Program/Staff Office*. Most Program Offices maintain workforces in both Washington, DC metropolitan area HQ Offices as well as in Field Organizations throughout the United States. Some Program Offices have personnel in several different locations, whereas others maintain staff in only one location.

2.2.2 Staff Offices

The 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. Due to their interaction with the intelligence community, the Office of Intelligence and Office of Counterintelligence have been excluded from this PWS. However, the Government reserves the right to issue task orders for IT support for Intelligence and Counterintelligence during the Contract period of performance. The 17 Staff Offices are as follows:

- Chief Information Officer (OCIO)
- Congressional & Intergovernmental Affairs (CI)
- Counterintelligence (CN) **(Excluded from the PWS)**
- Departmental Representative to the Defense Nuclear Facilities Safety Board (DNFSB)
- Economic Impact and Diversity (ED)
- Energy Assurance
- General Counsel (GC)
- Hearings and Appeals (HG)
- Independent Oversight & Performance Assurance (OA)
- Inspector General (IG)
- Intelligence (IN) **(Excluded from the PWS)**
- 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 Organizations support a single Program Office; however, some Field Organizations provide support to multiple Program Offices. Field Organizations take several forms including Operations Offices and Area Offices (including their respective subordinate sites), and Laboratories. The magnitude of each Field Organization is noted in the Technical Exhibits. The two (2) Naval Reactors, Rocky Mountain Oilfield Testing Center (Casper, WY), and Albany Research Center have all been excluded from the scope of this PWS. The majority of the IT work being performed at the Strategic Petroleum Reserve Office (SPRO), Carlsbad Area Office, and Richland Operations Office has also been excluded from the PWS because they currently receive IT support services directly from Managing and Operating (M&O) Contractors at their respective sites. However, the Government reserves the right to issue task orders for IT support at these excluded locations during the Contract period of performance. The SP shall manage Wide Area Network (WAN) connectivity to these sites.

2.2.4 National Nuclear Security Administration

The National Nuclear Security Administration (NNSA) is a semi-autonomous agency of DOE that focuses on administering policy in the area where energy and defense programs intersect. The mission of NNSA 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. EIA's sole purpose is to provide reliable and unbiased energy information.

The legislation governing EIA requires that it conduct its operations independently and in a manner that protects confidential information from unauthorized disclosure or use. EIA is therefore organizationally distinct from the remainder of DOE. Specifically, data or information acquired by EIA under a pledge of confidentiality and for exclusively statistical purposes can be used only by officers, employees, or agents of EIA. Disclosure or improper use of such information is a felony, with penalties up to and including imprisonment for 5 years, a fine of $250,000, or both. Any contractor employee who has access to or works on EIA IT resources must take the same security training and sign the same confidentiality statement on protecting confidential data as required of EIA employees.

The integrated EIA Mission Specific Data Systems are defined as all components that host data or on which data travels inside the EIA border perimeters, including but not limited to, desktops, workstations, and servers. E-mail, which is used by respondents to transmit confidential data to EIA, is also defined as a part of the EIA mission activity. Desktop support and assistance will be acquired through the consolidated DOE center. However, delivery of support and assistance requiring access to EIA Mission Specific Data Systems will be handled via an EIA support task as outlined above.

2.2.6 Power Marketing Administrations

The four (4) Power Marketing Administrations have been excluded from the scope of this PWS. However, the SP shall manage WAN connectivity for the Power Marketing Administrations. For more information, see http://www.energy.gov/engine/content.do?BT_CODE=OF_PMA.

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. Information on the IT users across DOE is presented in *TE 2-2: Users by Program/Staff Office* and *TE 2-3: Users by Physical Location*.

2.4 Work Locations

Workload to be performed by the SP under this Contract is required for both HQ Offices in the Washington, DC metropolitan area and in Field Organizations throughout the United States. More information on each location is presented in *TE 2-3: Users by Physical Location*.

2.5 Cross-Cutting Principles

The following categories represent IT activities that span the full scope of the PWS. The SP shall incorporate these principles in the work outlined in *Section 3: Performance Objectives and Measures*. These principles will guide the performance of all effort under the resulting Contract.

2.5.1 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 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 developmental systems for alignment with key business, technical, and operational goals. The SP shall support the development and execution of DOE's Enterprise Architecture.

The DOE Information EA Program:

- Implements a Department-wide EA to support the acquisition and maintenance of IT investments per the requirements of OMB Circular A-130, Information Technology Management Reform Act (ITMRA) of 1996 (a.k.a. Clinger-Cohen Act), CIO Council recommendations, 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

2.5.2 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 Clause C.2(h)*, Quality Assurance and Quality Control*. Specific quality requirements may also be provided at the individual task level.

2.5.3 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 clause C.2(b)(3), *Reporting & Records Maintenance,* and *Appendix B.1: Applicable DOE Directives and Orders* and *B.2: Other Applicable Directives and Orders*. See also: http:/cio.doe.gov/RBManagement/Records/records.html.

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

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 SP shall participate in and support the change control process and the Change Control Board (CCB). The discipline of Configuration Management applies to multiple tasks identified throughout *Section 3: Performance Objectives and Measures*. The SP shall be responsible for adhering to DOE configuration management standards, as directed by specific task orders, in the performance of this Contract.

2.5.5 Program/Project Management

DOE requires high quality, systematic program/project management as a factor in the accomplishment of planned program/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 COR determined are value added and necessary to achieve project success. This can be achieved by the SP identifying project management tools acceptable to the COR. 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 (M) 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 OMB Circulars: A-11, Part 7, Planning, Budgeting, and Acquisition of Capital Assets; A-109, Major Systems Acquisitions; A-123, Management Accountability and Control; A-127, Financial Management Systems; and A-130, Management of Federal Information Resources.

2.5.6 Certification and Accreditation

Many 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. For some systems and major applications, the SP must comply with additional certification and accreditation requirements as set forth in the specific task requirements.

The SP shall comply with DOE O 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
- 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 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
- More secure IT systems within the Federal Government

2.5.7 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 exclusive to the IT performance requirements under this PWS. The SP shall consider any intellectual, structural, or customer capital, that is understood, contained, or generated in the execution of any task order as KM information. The information held by the individuals responsible for such execution shall become shared non-exclusive intellectual property between the SP and DOE.

After reviewing the requirements of this PWS, the SP shall propose such a KM program. The SP shall propose, and use over the life of the resulting Contract, a KM tool to document information including but not limited to, costs, labor hours, output data, network statistics, enterprise architecture, cycle times, methodologies, processes, recommendations, solutions, and decision making rationale. Knowledge Management documentation will be detailed by the COR on a task order basis.

2.5.8 Reporting

Contract wide reporting requirements shall be in accordance with *DOE Form (F) 1332-1: Reporting Requirements Checklist*. Contract level reporting shall not be a separately priced line item but shall be included in the Offeror’s General and Administrative (G&A) expense rate or other indirect rate pool.

Individual reporting requirements below the master contract level will be established at the task level by the issuing organization. Unless specifically noted elsewhere in the PWS, task level reporting requirements will be established and funded at the task level.

3. Performance Objectives and Measures

The SP shall provide an enterprise solution regarding IT for DOE. The SP shall perform work in response to DOE-issued task orders. The SP shall perform the requirements listed herein in accordance with the instructions as noted in *TE: 3-2: Performance Requirements Summary (PRS)*, or as otherwise directed by individual task orders, which will determine requirements, adequacy, security, and reliability. The task 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

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 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 professional project management discipline, the Clinger-Cohen Act, Paperwork Reduction Act, Government Paper Elimination Act (GPEA), Computer Security Act, Presidential Decision Directive (PDD) # 63, the Government Performance and Results Act (GPRA), Section 508, and other applicable laws and regulations. The SP shall provide expert IT consultation and perform IT related work in response to business and mission needs at the various Program Offices, Staff Offices, and Field Organizations. All work will be further defined within the specific task orders issued.

IT Management tasks 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 EA recommendations; Capital Planning and Investment Control; Resource Management; Department Strategic Plans, according to the guidelines and initiatives, as put forward by the Secretary of DOE. SP work under the resulting 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 prepare, assist with the delivery, and maintain a record of briefings and presentations. The SP shall provide appropriate internal and external organizations information in the accomplishment of the overall IT mission. The SP shall be responsible for internal and external coordination to include, but not limited to, working with customers, other agencies, internal DOE Program/Staff Offices and Field Organizations, and other external entities. When requested, the SP shall provide relative information to assist in drafting responses to inquiries from Congress and other agencies.

3.1.1 Policy Development

The SP shall assist in the drafting and implementation of IT policy, directives, manuals, orders, procedures, SOPs, and guidelines, as required by individual task order, and submit 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 to include Program/Staff Offices and Field Organizations. The SP shall assist in the development and submission of the IT Strategy to the COR for approval in accordance with DOE directives and policies. The SP shall assist the Program Offices, Staff Offices, and Field Organizations 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 EA to the COR for approval. In addition, IT Standards shall be updated accordingly. The SP shall comply with DOE implementation of 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. The SP shall perform EA activities to include, but not limited to: promoting and implementing standard architectural practices; establishing an EA aligned with the Department's strategic goals facilitating an information exchange; ensuring the interoperability of business practices, systems, and technologies; defining and implementing a systems development life-cycle; architectural assessments and governance; and providing a framework for corporate systems modernization. The SP shall perform continuous analysis and make recommendations to the COR of areas to further analyze, consolidate, or otherwise align within DOE.

3.1.4 Capital Planning and Investment Control

The SP shall perform IT capital planning and investment control support activities in accordance with the IT Capital Planning Process. The SP shall perform work as directed by task orders in response to business needs to include, but not limited to, assisting the Program/Staff Offices and Field Organizations 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, assisting with developing Exhibit 300s (*Capital Asset Plan and Business Case)*, developing Exhibit 53s *(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 in response to specific task orders for the approval by the COR to include, but not limited to, assisting with efforts to: analyze and track budget expenditures; support the IT budget process; implement automated financial systems; track and coordinate resource 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 COR for review and approval.

3.1.6 Procurement Actions

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

3.1.7 Special Projects

The SP shall provide expert assistance in aiding the Government when Special Projects arise. Examples of Special Projects include, but are not limited to, I-Manage, E-Government, Public Key Infrastructure (PKI), and ad hoc projects as the requirements are identified by individual task orders.

Information Technology Management Performance Measures

The objectives set out above will have the following performance standards and expectations. The Performance Requirement Summary at TE-3.2 contains industry-standard measures at the contract level.

FAILURE TO MEET THESE EXPECTATIONS WILL RESULT IN THE SERVICE PROVIDER CORRECTING DEFIECIENCIES AT NO ADDITIONAL COST TO THE DEPARTMENT

Performance Standards	Quality Expectations
Completeness	All submissions will be 100% complete and compliant with all applicable regulations, DOE Orders and PWS section B.2.
Accuracy	All information submitted will be 100% accurate.
Effectiveness	All deliverables must contribute to the overall success of the PWS and Task Order
Timeliness	All deliverables will be on time and within schedule.
Cost	All tasks will be performed within the funding limit provided in each fully-funded Task Order.

3.2 Systems Development and 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 COR in response to task orders. All software and system changes shall be approved by the COR and may require approval by a CCB or other approval authorities as identified by individual task order. Systems development and engineering tasks include, but are not limited to, application development, software engineering activities, configuration management, web site development, and web site maintenance. The SP shall develop and maintain a documentation and code library.

3.2.1 Application Development and 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 include modernization and enhancements, to various software applications and data warehouses that support a variety of organizational and cross-organizational functions. 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 COR. The SP shall provide user training for developed or modified applications. The extent of user training required will be defined by the COR on a task order basis.

All work performed must conform to the requirements of the Clinger-Cohen Act or other applicable DOE Orders, DOE Corporate IM Guidance, DOE Software Engineering Methodology, OMB Circular A-130, the Joint Financial Management Improvement Program (JFMIP), and other applicable guidance. The SP shall identify its current SEI/CMM maturity level in its proposal. The COR, if appropriate, will specify the SEI/CMM level required by specific task order.

Existing applications shall be modified or enhanced per customer requirements as directed by task order 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 (except COTS), products and ownership to the Government at the end of each task order or the master contract, whichever arises first. Upon completion of each task order the SP shall comply with Department of Defense (*DOD) 8500.1 D: DOD Information Assurance* 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. Tasks include, but are not limited to, verification of hyperlinks, implementation of new technologies as they become available (e.g., multimedia, streaming technologies, and active server pages), and adherence to existing Federal regulations (e.g., Section 508). The SP shall assist DOE with various Government-wide initiatives, to include but not limited to, Web Council and e-Government. 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. These tasks include, but are not limited to, defining and developing of requirements (user and business), conducting testing, implementation, user training (on-site or remote), adherence to DOE EA Guidelines, and database design and maintenance, when applicable.

Systems Development and Engineering Performance Measures

The objectives set out above will have the following performance standards and expectations. The Performance Requirement Summary at TE-3.2 contains industry-standard measures at the contract level.

FAILURE TO MEET THESE EXPECTATIONS WILL RESULT IN THE SERVICE PROVIDER CORRECTING DEFIECIENCIES AT NO ADDITIONAL COST TO THE DEPARTMENT

Performance Standards	**Quality Expectations**
Completeness	All submissions will be 100% complete and compliant with all applicable regulations, DOE Orders and PWS section B.2.
Accuracy	All information submitted will be 100% accurate.
Effectiveness	All deliverables must contribute to the overall success of the PWS and Task Order
Timeliness	All deliverables will be on time and within schedule.
Cost	All tasks will be performed within the funding limit provided in each fully-funded Task Order

3.3 Information Technology Operations Support

The following subsections detail specific SP responsibilities pertaining to IT Operations Support within the DOE organization which includes sensitive, classified, and unclassified information systems. The SP shall be responsible for end-to-end operation of networks and IT assets, including, but not limited to: IT facilities management and IT physical security; telecommunications and network engineering services; network administration; network configuration, installation, maintenance, repair and upgrades; firewall management and maintenance; server administration; server installation, maintenance, repair and upgrades; system back-ups and restores; applications system administration; emergency preparedness; disaster recovery planning and execution; inventory control; maintenance, support, and service agreement management; audio, video, and web conferencing; user support/help desk; workstation management; wireless services; and voice and data services. 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 (Enterprise Solutions). All new software and hardware introduced to the network must meet all applicable guidelines and work in the current operating environment.

3.3.1 IT Facilities Management and IT Physical Security

The SP shall work with administrative services to provide facilities in use by the various IT department(s) with the proper power, heating, cooling, ventilation, lighting, space management, construction, security, and maintenance as appropriate for the various sites. The SP shall develop, implement, and test a backup and recovery strategy. 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 to include, but not limited to: creating timely notification of outages; maintaining physical security requirements and documents as deemed appropriate by the COR; and maintaining both physical and logical drawings of the processors, peripheral equipment, and their connectivity. The SP shall submit and seek approval for all IT related Configuration Change Proposals (CCP) with the CCB or the appropriate personnel, as identified by specific task orders. The SP shall also perform administrative management support functions as directed by specific task orders.

3.3.2 Network Administration

The SP shall perform networking activities pertaining to 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; providing network configuration management; establishing a testing environment; and installation, maintenance, repair, and upgrades of all hardware, firmware, software, and associated equipment that is installed as part of the network within DOE.

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

The SP shall provide 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 COR 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. The SP shall perform network functions include, but not limited to, firewall 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 submit and seek approval for all

IT related CCPs with CCBs or the appropriate personnel, as identified by specific task orders.

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 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/Staff Offices, Field Organizations, or the appropriate Federal cyber security officials 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.

3.3.2.3 Server Administration

The SP shall manage all production, test, and development servers. The SP shall perform server administration activities to include, but not limited to, account management, monitoring and auditing system logs, back up and recovery, security, managing operating systems, and storage management. The SP shall test and install operating system upgrades and patches in a timely manner consistent with security and change control requirements.

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 are maintained at the versions dictated by the EA. The SP shall meet certification and accreditation requirements as defined at the task order level. 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 update and maintain the KM solution accordingly. The SP shall coordinate and validate changes with application owners. The SP shall submit and seek approval for all IT related CCPs with CCBs or the appropriate personnel, as identified by the specific task order. The SP shall perform all non-emergency disruptive maintenance, repairs, and upgrades (i.e., network operating system upgrades, server refresh, etc.) during non-business hours or at the direction of the task orders. Non-business hours will be defined on a task basis.

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 restore and/or reproduce current and legacy systems, applications, and data in accordance with DOE management directives and requirements for data recovery or as specified by COR. The SP shall follow all DOE directives and requirements listed in *Appendix B: Technical Library* regarding off-site storage, restoration, and reproduction, including disaster recovery requirements.

3.3.2.6 Application Systems Administration

The SP shall maintain and provide reliable access to application systems to include, but not limited to: providing database administration services; hosting the application and ancillary software on servers; providing 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 test and install application upgrades and patches in a timely manner consistent with change control requirements. The SP shall perform day to day operational processing and fixes in a manner which meets the COR 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 determined at the task order level and maintain access logs.

3.3.3 Emergency Preparedness

The SP shall perform emergency preparedness activities to include disaster recovery planning and execution and development of the Continuity of Operations Plan (COOP).

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 individual task orders. The SP shall conduct and participate in test exercises as required by applicable Disaster Recovery Plans.

3.3.32 Continuity of Operations

The SP shall adopt existing and/or create COOPs. The SP shall execute, obtain approval, update, maintain, and test COOPs 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 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 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 excess GFP and support the COR in its disposal. For approved excess GFP this includes ensuring timely sanitation in accordance with DOD Directive (D) 8500.1 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 manage maintenance and support agreements for hardware and software as specified by specific task orders. The SP shall ensure that all such agreements are registered with the provider in the name of DOE. The COR 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 include, but are not 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 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 COR.

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 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 COR 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/Staff Offices and numerous Field Organizations, nationwide, and provide analysis of the usages by organization on a monthly basis. As required by specific task orders, 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. The SP shall perform scheduling functions to include, 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 provide services that meet Federal and general commercial standards as set forth in specific task orders.

3.3.7 User Support and Workstation Management

The SP shall provide user support and workstation management as described in the following subsections.

3.3.7.1 User Support

The SP shall be responsible for Customer Relationship Management (CRM), to include, but not limited to, pre-service activities, during service activities, post-service activities, and customer feedback program to include surveys, follow-ups, and liaison with the customer. The SP shall provide user support as defined at the task level, to include, but not limited to, help by telephone, remote control, and support at the desktop/problem area. The SP shall support DOE requirements for remote access. 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, 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 develop self-help training aids (e.g., tips & tricks, FAQ’s) for recurring problems as needed or required.

3.3.7.2 Workstation Management

The SP shall perform workstation management to include, but not limited to, planning, design, testing, 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. The SP shall provide and maintain a COR approved refresh rate; perform PC adds, moves, and changes; load clients; provide central management and remote management of desktops; and provide loaner equipment. The SP shall research, apply, distribute, and document desktop patches and service packs.

3.3.8 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 and report findings based on the analysis to the COR.

3.3.9 Voice and Data Services

The SP shall plan and 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 systems, 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. The SP shall update and maintain the KM solution accordingly.

As applicable, the SP shall monitor, operate, and maintain a telecommunications management system for customers including, but not limited to, conducting user unit 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.

Operations Support Performance Measures

The objectives set out above will have the following performance standards and expectations. The Performance Requirement Summary at TE-3.2 contains industry-standard measures at the contract level.

FAILURE TO MEET THESE EXPECTATIONS WILL RESULT IN THE SERVICE PROVIDER CORRECTING DEFIECIENCIES AT NO ADDITIONAL COST TO THE DEPARTMENT

Performance Standards	**Quality Expectations**
Completeness	All submissions will be 100% complete and compliant with all applicable regulations, DOE Orders and PWS section B.2.
Accuracy	All information submitted will be 100% accurate.
Effectiveness	All deliverables must contribute to the overall success of the PWS and Task Order
Timeliness	All deliverables will be on time and within schedule.
Cost	All tasks will be performed within the funding limit provided in each fully-funded Task Order.

3.4 Cyber Security

The SP shall perform cyber security functions in accordance with DOE O 205.1 to include, but not limited to, cyber resource protection, risk management, program evaluation, cyber security plan development and maintenance, auditing, and network intrusion detection. Cyber security is the protection of IT 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, availability, and authentication of DOE IT systems. Integrity requires guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. Confidentiality requires preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information. Availability requires ensuring timely and reliable access to, and use of information and information systems. Authentication requires that messages come from the stated source.

3.4.1 Cyber Resource Protection

The SP shall provide cyber security for DOE in compliance with DOE O 205.1 and DOE Cyber Security Management Program, dated March 21, 2003, and any other applicable security regulations and policies. In the case of the NNSA, the SP shall comply with all NNSA Policy Letters concerning cyber security.

The SP shall protect all DOE unclassified and classified information and information systems under its management. The Designated Approval Authority(s) (DAA) will define at the task level, the level of risk DOE is willing to accept. 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 DOE in compliance with Federal cyber security directives and best business practices. The SP shall also provide the relevant Cyber Security awareness training as directed at the task level.

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 security and network support services 24 hours a day, seven days a week, to include, but not limited to, responding to real or potential security events, responding to Federal data calls or other mandated reporting requirements, and providing after-hours security support for DOE networks and all associated Program/Staff Offices and Field Organizations.

The SP shall oversee response(s) to all incidents involving malicious or suspicious code to include, but not 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 update and maintain the KM solution accordingly. 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 at the desktop, remote locations, and at home. The SP shall also provide reports of virus encounters on a monthly basis to the DOE CIAC, to various virus bulletins, 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). 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 perform risk analysis and implement a COR 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, on IT systems, as required by DOE to ensure it meets DOE's requirements.

Cyber Security Performance Measures

The objectives set out above will have the following performance standards and expectations. The Performance Requirement Summary at TE-3.2 contains industry-standard measures at the contract level.

FAILURE TO MEET THESE EXPECTATIONS WILL RESULT IN THE SERVICE PROVIDER CORRECTING DEFIECIENCIES AT NO ADDITIONAL COST TO THE DEPARTMENT

Performance Standards	Quality Expectations
Completeness	All submissions will be 100% complete and compliant with all applicable regulations, DOE Orders and PWS section B.2.
Accuracy	All information submitted will be 100%

	accurate.
Effectiveness	All deliverables must contribute to the overall success of the PWS and Task Order
Timeliness	All deliverables will be on time and within schedule.
Cost	All tasks will be performed within the funding limit provided in each fully-funded Task Order.