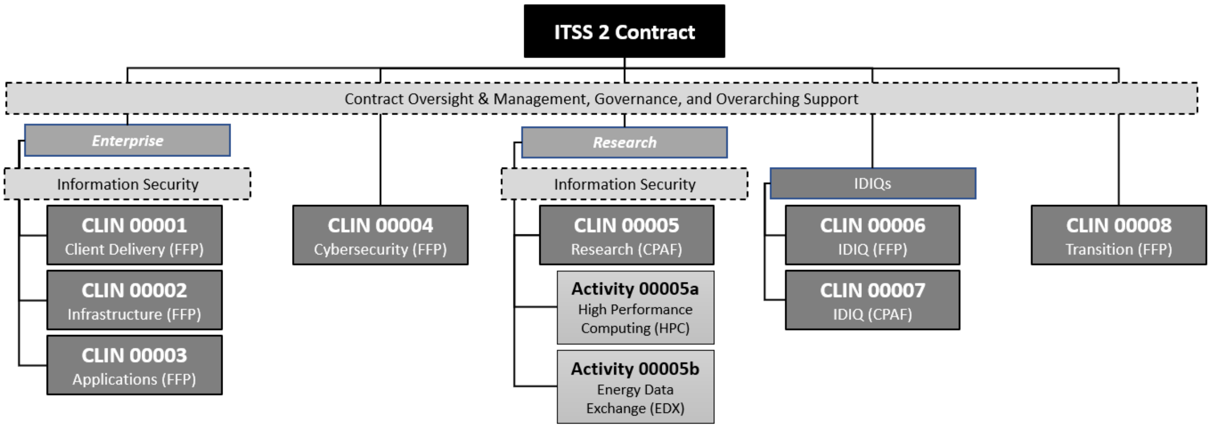
Performance Work Statement (PWS)
Information Technology Support Services 2 (ITSS2)

1 INTRODUCTION

1.1 Contract Structure

The National Energy Technology Laboratory (NETL) requires Information Technology Support Services (ITSS2) to enable the laboratory to fulfill its role in supporting the Department of Energy's (DOE) mission. These services are to provide capabilities including requisite experience, skills, and personnel to maintain, operate and integrate information technology (IT) solutions for Enterprise, Cybersecurity, and Research. The specific contract structure consists of contract line items (CLINs) shown in the diagram below:



1.2 Background

NETL is operated by the DOE Office of Fossil Energy and Carbon Management (FECM) whose mission is to drive innovation and deliver solutions for an environmentally sustainable and prosperous energy future by ensuring affordable, abundant, and reliable energy. All NETL activities support the DOE mission to ensure America's security and prosperity by addressing its energy, environmental and nuclear challenges through transformative science and technology solutions. NETL is the only national laboratory that is government-owned, and government-operated by DOE. It conducts and manages research activities at its sites in Pittsburgh, Pennsylvania (PA); Morgantown, West Virginia (WV); and Albany, Oregon (OR). It also maintains a satellite office in Houston, Texas (TX). NETL's project portfolio includes research and development conducted through partnerships, cooperative research and development agreements, financial assistance, and contractual arrangements with universities and the private sector.

The innovations NETL and its partners discover address a range of FECM challenges, including carbon dioxide capture, utilization, and storage; advanced coal processing; enhanced natural gas exploration and production; next-generation emissions controls; production of materials for extreme environments; and high-efficiency boilers, turbines, fuel cells, and other power systems. NETL also manages DOE projects that tackle emerging issues in renewable energy, Smart Grid implementation, and ways to improve the reliability and efficiency of both existing and future power plant and electricity delivery systems.

NETL is comprised of six organizational offices including the Office of the Director, Science and Technology Strategic Plans and Programs office, Research and Innovation Center, Technology Development Center, Laboratory Operations Center, and the Finance and Acquisition Center, totaling approximately 1,400 personnel. The largest sites are in Morgantown, WV and Pittsburgh, PA with approximately 650 personnel in each location. The Albany site has approximately 100 personnel.

1.3 Contract Purpose

This contract is to obtain quality professional IT services of the caliber necessary to meet the business and research needs of a world class laboratory. The intent is not only to obtain reliable, high quality IT support services, but to also acquire a business partner who has the capabilities to ensure NETL's success and continuous improvement.

The services delivered must align IT resource expenditures with business goals and objectives and facilitate an IT environment which is responsive to organizational requirements. The personnel who support NETL through this contract are required to be both professional and knowledgeable, with the necessary experience and skills to maintain and operate the NETL IT environment and integrate future upgrades, enhancements, and developments.

1.4 Business Operating Hours

NETL has three primary campuses and one satellite office, which are located in three different time zones (i.e., Eastern Standard Time, Pacific Standard Time, and Central Standard Time). NETL's business hours are defined as Monday through Friday from 7 A.M. through 5 P.M. local time for each campus.

1.5 Oversight and Management

1.5.1 Program Manager

The Contractor shall provide a Program Manager to serve as the Contractor's authorized supervisor for technical and administrative performance of all work. The Program Manager shall receive and execute, on behalf of the Contractor, such technical directions as the DOE Contracting Officer's Representative (COR) may issue within the terms and conditions of the contract.

The Program Manager's primary responsibility is to ensure efficient operations of the ITSS2 contract in support of NETL IT initiatives, and specifically

- Ensure overall productivity and operational effectiveness through continuous improvement and utilization of resources and assets.
- Ensure compliance with federal government regulations and mandates.
- Ensure flexibility and agility of systems to adapt quickly and cost-effectively to support changes in business mission and operational environment.
- Prevent IT obsolescence, reduce IT maintenance & operations costs, and free-up budget resources for investing in new IT projects and capabilities.

The Contractor's employees are accountable solely to the Program Manager, who in turn is responsible for performance to the Government.

1.5.2 Business Manager

The Contractor shall provide a Business Manager to provide finance, accounting, and procurement management for the ITSS2 contract. Responsibilities include, but are not limited to:

- Manage the contract in conjunction with the Program Manager.
- Establish, track performance, and pay subcontracts.
- Manage the Cost Management Report (CMR).
- Manage Financial and Accounting Reporting.
- Build and maintain a procurement process; procure materials and services in support of IT initiatives.

1.5.3 Contract Personnel

The Contractor shall provide a stable, competent work force to meet the requirements of the contract. The Contractor shall ensure that its contract personnel, over the contract life, know and understand DOE/NETL's organizational structure, its mission, its policies, and its IT environments. Employees shall remain technically current in their fields of expertise in order to effectively perform duties of their positions.

The Contractor shall have access to highly specialized business, management, and technical IT expertise that, due to the specificity of the tool, technology, or business practice; may require skills, knowledge, or specific technical expertise that the Contractor may not have within its available resources. In these instances, the Contractor may acquire temporary short-term resources through other means if approved by the Contracting Officer (CO). The Contractor shall have quick and expedient access, not to exceed 30 days, to specialized technical and business management consulting capabilities.

2 GENERAL CONTRACT REQUIREMENTS

The following subsections detail specific Contractor responsibilities pertaining to Governance and Overarching Support. The Contractor shall provide consistent practices within these areas of support across all contract line-item numbers (CLINs,) while adhering to NETL’s established processes, procedures, and tools.

Note: All applications, systems and networks covered by this contract are owned by the federal government; therefore, the Government shall be the final approving body for granting privileged access. The Government has the right to access all IT systems supported by the Contractor.

2.1 Governance

The Contractor shall follow Federal Civilian standards and processes, for operating and maintaining all IT systems, applications, and projects under the purview of the contract. It is expected that the Contractor shall use industry standard best practices, to include Information Technology Infrastructure Library (ITIL) and Capability Maturity Model Integration (CMMI) as a core foundation for executing these governing processes.

The Contractor shall follow the governance framework established by NETL, described in this section, to include Quality Management; Standard Operating Procedures (SOPs); Risk Management; Change Management; Configuration Management; Knowledge Management; Project Management; Operational & Maintenance (O&M); Work Management; Incident, Problem and Monitoring & Event Management; and IT Asset Management. The Contractor shall manage according to this governance framework to ensure that the IT organization operates in an effective, efficient, and compliant fashion.

Any changes to the computing environment that impact architectural designs, shall be reviewed with the Information Technology Architecture Board (ITAB), a body comprised of Federal architects and senior IT personnel.

2.1.1 Quality Management

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 Contractor to provide an IT Contractor organization which performs at the highest level of quality. The Contractor shall establish a quality element within its organization that ensures compliance with applicable Federal mandates, contractual performance standards, and industry standards and best practices. The Contractor shall provide a Quality Assurance Management Plan (QAMP) to deliver quality services under the contract which will be reviewed by the Government annually.

2.1.2 Standard Operating Procedures

The Contractor shall be responsible for maintaining and adhering to NETL's SOPs to ensure an effective operating environment. The Contractor shall contribute in drafting and implementation of NETL's IT policies, directives, manuals, orders, procedures, SOPs, and guidelines, as required.

2.1.3 Risk Management

The Contractor shall follow the Risk Management Framework (RMF) as established by the National Institute of Standards and Technology (NIST) Special Publication 800-37, "Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy" as the standard assessment and authorization (A&A) process. The Contractor shall incorporate NETL's Risk Management processes for the initiation of IT risks and issues including mitigation, acceptance, and closure through the Risk Review Board (RRB). The Government's role within the RRB will be to direct and disposition risks and mitigations to meet the stability, security and privacy requirements for the system and organization.

2.1.4 Change Management

NETL continuously aligns with evolving IT industry best practices, the changing application of IT in the workplace, and Federal mandates. The Contractor shall use standard methods and procedures for handling all changes to applications, systems, networks, and services within the IT environments. All changes shall be performed in accordance with NETL IT SOPs with government authorization through the Change Advisory Board (CAB), a standing governance body that oversees change led by the Contractor.

The Contractor shall maintain integrity, traceability, and control over change throughout systems, hardware, and application lifecycles through the establishment of a 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.

2.1.5 Configuration Management

The Contractor shall be responsible for the configuration management of all IT assets including but not limited to servers, desktops, databases, operating systems, networking, applications, and software, to maintain knowledge and control of how these IT assets are configured and how they relate to one another. The Contractor shall maintain and keep the Configuration Management Database (CMDB) up to date at all times. The Contractor shall assist NETL in the improvement and adherence of Configuration Management processes.

2.1.6 Knowledge Management

It is the intention of NETL to use Knowledge Management (KM) to develop and improve IT control, efficiency, and effectiveness. The Contractor shall be responsible for curating, analyzing, creating, organizing, storing, using, and sharing knowledge that exists within the IT organization. The Contractor shall manage information for NETL IT services, applications, platforms, databases, and infrastructure, including but not limited to troubleshooting guides, user instructions, training materials, project management artifacts, architectural diagrams and documentation, system and network diagrams, known error database (KEDB), CMDB, change management records, methodologies, processes, SOPs, system and network statistics, solutions, and decision-making rationale.

2.1.7 Project Management

NETL requires high quality, systematic project management as a factor in the accomplishment of planned project objectives and the realization of projected benefits. The Contractor shall be responsible for the day-to-day management of indicated IT projects and Operations & Maintenance (O&M) work by delivering the means, methods, and resources to meet the contract end point requirements and the intermediate requirements that the COR determines are value added and necessary to achieve project success. The Contractor shall ensure a seamless operating environment throughout the lifecycle of this contract, including transition activities, when the Contractor is directed to or plans to introduce new technologies and functions. The Contractor shall scope, govern, manage, and resource assigned projects via the existing enterprise work management platform.

2.1.8 O&M Work Management

The Contractor shall document and transparently communicate all O&M efforts occurring across all CLINs. Work management ensures the Government understands the scope of the effort, planned schedule, team responsible, and priority to assist with resource capacity planning. Historically, NETL's enterprise work management system has provided capabilities to manage tasks effectively throughout the contract which can continue to be matured and improved by the Contractor.

2.1.9 Incident, Problem and Monitoring & Event Management

The Contractor shall address incidents within established NETL guidelines and shall provide incident management, problem management, and monitoring & event management. The requirements shall include, but are not limited to:

- Participate in the **Incident Management** process, to resolve and close escalated incident tickets within the appropriate amount of time as detailed by Government approved Service Level Agreement (SLA), and to regularly update user and incident tickets with troubleshooting actions, diagnosis of problem, and resolution actions.
- Identify issues, troubleshoot, and repair, coordinate, and escort external service providers; coordinate the shipment of equipment for repair, and track returned equipment.
- Maintain and mature the knowledge base of problem resolutions that are related to service requests and inquiries while keeping the knowledge base solutions up to date and applicable to all applications and facilities.
- Participate in the **Problem Management** process, to investigate and analyze the causes of problems, develop workarounds, and recommend longer-term resolutions.
- Perform root cause analysis for all IT service outages or significant degradation and document the results in a Service Interruption Report (SIR) within 5 days of the event.
- Initiate vendor support requests including but not limited to; warranty claims, technology specific support, obtaining spare/replacement parts, and returning defective systems or components to manufacturer in accordance with manufacturer's disposition instructions.
- Participate in the **Monitoring and Event Management** process, to ensure applications, systems and networks are continuously monitored and to enable rapid service restoration of IT services resulting from negative changes in the IT environment, thereby minimizing business disruptions and security risks.

2.1.10 IT Asset Management

The Contractor shall be responsible for planning and managing the lifecycle of all IT assets at NETL, where the requirements shall include, but are not limited to:

- Ensure software compliance and license management as well as warranty tracking such that all production hardware and software is always within the original manufacturer's equipment warranty or under vendor support maintenance agreement, as well as recording and tracking license distributions to ensure compliance.
- Record and track all IT assets throughout their lifecycle in NETL's IT Asset Management Tool and in accordance with the NETL IT SOPs, as part of IT inventory.

- Manage spare-parts inventories (as required to minimize equipment repair time) including but not limited to Data Center systems, spare hard drives for servers, telecommunications equipment and peripheral components and computers, computer components, and peripheral components for on-site replacement. Parts, supplies, and equipment required for on-site repairs will typically be purchased by the Government.
- Maintain an IT asset roadmap to track End-of-Life (EOL)/End-of-Support (EOS) and provide recommendations and plans for replacements/upgrades to the Government, at least 24 months before the EOL/EOS dates.
- Ensure EOL systems, applications and/or components are properly decommissioned, including removal of any data on equipment and updating all associated configuration items (CIs).

2.2 Overarching Support

The following subsections detail specific functions which the Contractor will be required to perform across all CLINs within the contract. These subsections consist of Architectural and Design Support Services, Procurement Support, Cybersecurity Hygiene Support, and support for Data Calls and Mandate Responses. The Contractor shall provide support in each of these areas consistent with established federal processes and procedures.

2.2.1 Architecture and Design Support Services

The Contractor shall provide architectural support to research, develop, analyze, and recommend best practice and guidance for NETL's IT environments—on-premises or cloud—upon request. The requirements shall include, but are not limited to:

- Support engineering activities to design and architect new IT systems, applications, and approaches.
- Support annual planning, which includes providing a consolidated view of current and future architectures.
- Support the development of business cases, alternative analyses, technical requirements, rough orders of magnitude for labor and costs, and technical specifications.
- Support IT service mapping activities, including development and maintenance of baseline configuration of systems, applications, software, and operational interdependencies.
- Suggest new initiatives and innovative approaches to maintain NETL at the cutting edge of IT technological capability.
- Participate and contribute to cybersecurity risk management framework and information system authorization processes including A&A package artifacts.
- Present to the ITAB as necessary so that all major initiatives are approved across the entire NETL IT environment to avoid negative impacts to operations and research.
- Be responsible for the integration of all systems and components that become part of the NETL IT production environment, whether purchased/developed internally through the IT organization or purchased/developed by another group within NETL to ensure accessibility, availability, security, and integrity.

2.2.2 Procurement Support

The Contractor shall assist as required in the procurement of a variety of IT products and services. The Contractor shall adhere to all procurement guidelines including, but not limited to, Federal Information Technology Acquisition Reform Act (FITARA) and Federal Risk and Authorization Management Program (FedRAMP). Specific procurement actions include, but are not limited to, preparing all related articles of the procurement package; assisting in the completion of any FITARA paperwork; assisting in the completion of any non-standard hardware forms; submitting purchase requisitions into the DOE Strategic Integrated Procurement Enterprise System (STRIPES); researching products and services; conducting cost estimates; requesting vendor quotes; recommending and validating specifications; and verifying the receipt of procured items. Procurement actions may be required under any of the contract CLINs and may consist of, but not be limited to, the purchase of hardware, software, firmware, materials, leases, license agreements, and maintenance agreements. For renewal of those maintenance agreements that are processed/managed by the Contractor for the Government, the submission into STRIPES should occur no less than 60 calendar days before the expiration date.

2.2.3 Cybersecurity Hygiene Support

The Contractor shall conduct periodic and recurring cybersecurity hygiene activities across all contract CLINs per the NIST 800-53 control set adopted by NETL. The purpose of cybersecurity hygiene is to ensure the safe handling of critical data, ensure that all applications, systems, and networks are secure, and to proactively address risk. The Contractor shall ensure the confidentiality, integrity, and availability of data generated by IT systems and support the assertion that systems operate as intended and that output is reliable. The Contractor shall establish and implement a baseline of practices and controls for managing the most common and pervasive cybersecurity risks NETL may face. The requirements shall include, but are not limited to:

- Establish and maintain system and network security and monitoring.
- Adhere to logical access policies, standards, and processes to manage access based on business need and on least privilege when maintaining user accounts, limiting the number of users with administrative access.
- Transition to role-based access and deny privileged access unless explicitly permitted.
- Target and implement multi-factor authentication for privileged access for all environments.
- Practice physical security to ensure the physical security of IT from individuals and environmental risks.
- Manage technology changes and use standard, known-secure, approved-baseline configurations.
- Implement controls to protect and recover data.
- Decommission and retire unused servers, services, ports, and devices in alignment to SOPs.
- Perform vulnerability, malware, and threat monitoring and remediation.
- Adhere to source code/document version control procedures to protect the integrity of program code.
- Ensure the complete and accurate processing of data, from input through output.
- Ensure the privacy and security of data transmitted between applications.
- Ensure knowledge of cybersecurity processes and targeted controls to avoid unnecessary delays in execution.

2.2.4 Data Calls and Mandate Responses

The Contractor shall take the appropriate actions to assist with response to Government Data Calls and Federal Mandates. These data calls can originate from numerous sources, both internal and external to NETL such as the DOE Office of FECM; the DOE Chief Information Officer (CIO); the DOE Inspector General; the NETL Director, the NETL Chief Operations Officer (COO); as well as other directorates within NETL. The Contractor shall be prepared to support IT-related data calls, spanning all CLINs of the contract.

The Contractor shall assist in responding to data calls and mandates as directed by the Government. Examples of data calls include, but are not limited to the following:

- Responding to and/or implementing Executive Orders, Office of Management and Budget (OMB) Memoranda and Department of Homeland Security (DHS) Binding Operational Directives (BOD).
- Supporting the compilation and maintenance of information to develop responses to cybersecurity related data calls or investigations.
- Conducting periodic audits to verify and validate 800-53 security controls, Federal Information System Modernization Act (FISMA) compliance, information security, and Authority to Operate (ATO)/Authority to Use (ATU) status.
- Responding to internal and external licensing audits.

3 ENTERPRISE (CLINs 00001-00003)

3.1 Background

3.1.1 General

Enterprise services (CLINs 00001-00003)—including Client Delivery (Service Desk Support, Meeting Room Support, and Endpoint Support), Infrastructure (Data Centers, Networks, Telecommunications, and Client Services Engineering), and Applications with support from Solutions Engineering—are delivered as needed across the Enterprise environment which consists of NETL's business network (Admin LAN) and research networks (Research LAN and Science LAN).

The business network (Admin LAN) provides users with access to a standard Windows client operating system; commercial off-the-shelf (COTS) applications; and Microsoft Office 365 cloud-based software-as-a-service (SaaS) solution for email, collaboration tools, and Microsoft Office productivity tools. Admin LAN manages a Citrix XenApp platform designed to support 360 concurrent users, which provides secure remote access to NETL applications. The Citrix environment includes 12 servers across Pittsburgh, Morgantown, and Albany, hosted on-premises. Admin LAN manages approximately 1,700 PCs (Laptops and Desktops), 300 Network Printers, and 400 wireless devices (iPhones and iPads).

The research local area network (LAN) infrastructure (Research LAN) provides NETL researchers and their collaborators with access to mission critical instrumented control systems (ICSs) and software. These ICSs allow researchers to control projects from a computer console and record data for later analysis leading to publication. Research manages a Citrix XenDesktop Remote Desktop platform designed to handle 10-20 concurrent users. Research LAN utilizes standard Windows operating systems. Research LAN manages approximately 270 endpoints and 550 users.

The scientific LAN infrastructure (Science LAN) provides NETL researchers and their collaborators with access to mission critical, computational research platforms (hardware and software resources) and state-of-the-art post-processing and visualization capabilities. Science LAN manages the Virtual Engineering Environment (VEE) which is designed to support 60-70 concurrent users. Science LAN utilizes Linux operating systems, Windows operating systems, virtual desktops hosting Windows, and custom-configured applications. Science LAN manages approximately 370 endpoints and 150 users.

Strategic plans for efficiency call for the consolidation of the research networks. It is anticipated that the Research LAN services will be decommissioned and services currently on that LAN will be disbursed to the Admin LAN, Science LAN, cloud, and other locations as deemed appropriate. The Contractor shall be responsible for all work associated with implementing the consolidation of research networks.

3.1.2 Networks

The three main NETL sites—Albany, Morgantown, and Pittsburgh—are interconnected by two network circuits at each site Department of Energy Network (DOENET) and Energy Sciences Network (ESNET), configured in a redundant architecture; the networks provide site-to-site connectivity and external network connectivity including DOE networks, Public Cloud Service Providers, and Internet/Trusted Internet Connection (TIC) services. The internal network comprises a collection of segmented Virtual Local Area Networks (VLANs) which are supported by approximately 500 physical network devices across NETL, and includes but are not limited to switches, routers, firewalls, and wireless access points.

3.1.3 Datacenter Facilities

NETL currently has five production on-premises data centers which house IT assets for both Enterprise and Research. Three of the five data centers are shared across all environments and are managed by Enterprise.

The other two data centers are dedicated to Research's Supercomputer and Artificial Intelligence/Machine Learning (AI/ML) computing environment and are managed by Research *[CLIN 00005]*.

Enterprise's on-premises hosting environment is comprised of approximately 500 servers which include production, test, and development systems, where more than 90% of these systems have been virtualized. These servers host various IT services and applications including but not limited to directory services, file services, backup services, print services, facilities services, database services, and application services. NETL's IT strategy aims to maximize cloud-based IT services for Admin LAN workloads, with a goal of shifting at least 70% to cloud in the next five years.

3.1.4 Telecommunications

Telephony/Voice over Internet Protocol (VoIP) Services are based on Cisco's Unified Communication solution, hosted on-premises at Albany, Morgantown, and Pittsburgh; there are approximately 40 virtual servers in total. The VoIP services access the Public Switched Telephone Network (PSTN) though Session Initiation Protocol (SIP) trunks at each site. There are approximately 2,500 endpoints deployed across the laboratory; the range of endpoints include the Cisco VoIP phones and analog endpoints via voice gateway devices. NETL maintains DOE Headquarters (HQ) accounts for priority access to telecommunication services (Government Emergency Telecommunications Services (GETS), Wireless Priority Services (WPS)), in the event of a major service disruption. NETL also maintains DOE HQ accounts for priority service restoration (Telecommunications Service Priority (TSP)).

Audio/Video (A/V) Services are delivered to approximately 60 conference rooms across the laboratory which include: conference centers for all employee meetings; program reviews and training; executive Video Teleconferencing (VTC) rooms with advanced features and control systems; three Visualization Laboratories, 35 rooms with VTC systems; and standard meeting rooms with projectors and or video displays. In addition, NETL has locations with displays (for commercial TV, NETL information, etc.) at Albany, Morgantown, and Pittsburgh.

The NETL Radio Frequency Program maintains and operates Land Mobile Radio (LMR) systems at Albany, Morgantown, and Pittsburgh for use by NETL's Facilities and Engineering Team; the Environmental, Safety and Health Team; the Security and Emergency Response Organization Team; and Research. NETL operates handheld (portable) radios, mobile (vehicle mounted) radios, base station (mobile with AC power supply) radios, and seven repeaters. NETL LMR systems operate on federal spectrum assigned and managed by the National Telecommunications and Information Administration (NTIA). NETL LMR systems operate in the Very High Frequency (VHF) band (Albany) and Ultra-High Frequency Band (Morgantown and Pittsburgh). NETL maintains a contract with Mission Support and Test Services LLC (a Nevada National Security Site (NNSS) contractor) to process NETL requests for radio frequency licenses, renewals, modifications, or terminations. Strategic business applications are enabled from the core underpinnings previously noted above and are the path to leveraging resources effectively for higher order actions, moving NETL into the future.

3.1.5 Applications

Enterprise Applications include the maintenance and support of approximately 90 hosted systems with varying levels of support including direct software development, platform administration, deploying on behalf of other solution providers, patching procured products, and performing as an intermediary to new and existing NETL software vendors. In support of application services, Enterprise database management includes platform administration, database administration, database design, development, and customer support for approximately 19 structured query language (SQL) Server Standard instances, 4 SQL Server Enterprise clustered environments with AlwaysOn failover, and 2 Oracle Database Appliances hosting a collection of Oracle 19c schemas.

Enterprise business intelligence and data analytics includes platform administration, data modeling, report creation, storytelling, and dashboarding in support of the enterprise applications and data primarily utilizing Cognos Analytics and Tableau Server. NETL IT's strategy aims to maximize cloud managed services for applications, services, database management, and business intelligence using Platform-as-a-Service (PaaS) and SaaS offerings where available and feasible which could include technological shifts and dependencies on particular vendors.

3.2 Scope

The Contractor shall provide capabilities including experience, skills, and personnel to maintain, operate, and integrate IT solutions for Enterprise, which includes Client Delivery, Infrastructure, Applications, and Solutions Engineering.

The Contractor shall be responsible for information systems security functions for all activities under CLINs 0001-0003. The requirements shall include, but are not limited to:

- Analyze design constraints, trade-offs, and detailed system security.
- Serve as a principal advisor on all matters, technical and otherwise, involving security controls for each system.
- Understand the unique characteristics and requirements of the research networks so that appropriate cybersecurity remediations can be suggested and applied to allow research within a safe environment.
- Assist in the development of the system-level security, which may include, but is not limited to, physical and environmental protection; personnel security; incident handling; and security and privacy training and awareness of both system owners and IT support staff.
- Lead, organize support, execute, and directly contribute to the RMF A&A packages for all enterprise systems, subsystems, and environments in collaboration with their respective system owners.
- Document any modification or deviation from organizationally defined security policies and standards (i.e., FISMA, NIST, etc.) as well as the resulting risks and any recommended mitigation actions for Authorizing Official (AO) or Authorizing Official Designated Representative (AODR) approval.
- Protect information and information systems from unauthorized system activity or behavior to provide confidentiality.
- Contribute to Disaster Recovery for systems under development and ensure testing prior to new systems entering a production environment.
- Function as the focal point and interface with Government Cybersecurity staff and third-party assessors as needed on all incoming cybersecurity issues, mandates, data calls, audits, and assessments.
- Interface with Government Architects and Contractor architect support personnel to ensure security control integration into overall system designs.

3.3 CLIN 00001 – Client Delivery

3.3.1 CLIN Type

This CLIN is firm-fixed price.

3.3.2 Place of Performance

NETL employees are primarily located in Morgantown, Pittsburgh, Albany, and work remotely; therefore, it is expected that staff will be available to support customers both onsite and remotely within the hybrid work organization. For operations and maintenance actions requiring hands-on work or in-person Customer interaction, the place of performance for this CLIN is at NETL primary sites in Albany, OR, Morgantown, WV, and Pittsburgh, PA.

3.3.3 Objectives

The objective of this CLIN is to provide client-facing technical support services to the NETL user community.

3.3.4 Scope

This CLIN encompasses all client-facing technical support services for the NETL user community including service desk, meeting room support, and endpoint support, where activities are primarily focused on Incident Management, Request Fulfilment, and Problem Management.

The Contractor shall provide NETL with all supervision, personnel, tools, equipment, and services (excluding those items identified under the Government-furnished section of the contract) to satisfactorily perform the Client Delivery services identified in this CLIN. It is expected that the Contractor shall perform in accordance with the specified SLAs.

3.3.5 Requirements

The Contractor shall perform all work within this CLIN according to the requirements specified in *General Contract Requirements [2.0]*. The Contractor shall provide Service Desk, Meeting Room Support, and Endpoint Support services.

Service Desk

The Contractor shall provide technically knowledgeable, courteous, and responsive first contact support to supply rapid resolutions to user incidents (which include events that cause or may cause an interruption or reduction of service), requests for information (including how-to instructions), and requests for NETL IT services. The requirements shall include, but are not limited to:

- Be available to support employees through walk-in, a single phone number, online portal, or chat, during business operating hours as applicable.
- Monitor additional research phone numbers and emails for service requests.
- Respond (either by phone call or email) to the customer acknowledging receipt of the request within 1 business day of a customer's request if the initial request was not verbally given person-to-person.
- Triage the customer's actual need properly, prioritize the issue accurately, and assign the trouble ticket to the appropriate support personnel for remediation to prevent trouble tickets languishing in the wrong support area.
- Provide support for Government Furnished Equipment (GFE) computers and NETL supported applications of employees working onsite or remotely, either by phone or remote desktop administration. Issues which cannot be resolved remotely will require coordination with the user to return equipment to a NETL site for additional troubleshooting.
- Facilitate and support the shipment of IT equipment to and from remote US worker locations.
- Record, assign, and track all support calls to the Service Desk per NETL policies for incident management using Government-provided tools *(Governance [2.1])*; maintain and update workflow status information for accuracy to make the information—such as description of the fix action; estimated time of completion; and responsible point of contact—available to NETL customers.
- Regularly update user and trouble tickets with troubleshooting actions, diagnosis of problem, and resolution actions.
- Provide weekly customer email updates until resolution is complete.
- Resolve and close trouble tickets within the appropriate amount of time as detailed by an NETL approved SLA.

- Establish and maintain a documented knowledge base of problem resolutions that are related to service requests and inquiries; keep the knowledge base solutions up to date and applicable to all applications and facilities. It is expected that the Contractor shall utilize the knowledge base to guide users through resolution of the reported issues.
- Provide Tier 1 technical support, such as resetting passwords, diagnosing issues for supported hardware, software, applications, and services, and providing basic hardware/software support while utilizing the knowledge base of documented fix actions, lessons learned, industry practices, and standards of troubleshooting. Issues which cannot be resolved by the Service Desk (either by phone or by remote desktop administration) shall be forwarded and escalated to the appropriate technical support area for action.
- Provide desk-side support for all applicable building locations whenever necessary to resolve incidents or implement service requests in accordance with SLAs.
- Perform problem management (including trend analysis to identify recurring incidents and necessary changes), customer training, and IT service management (ITSM) improvements.
- Provide timely notifications to users and appropriate Government points of contact (with prior Government approval) of planned and unplanned outages of systems, networks, and other major components using Government approved tools and communication methods.
- Prioritize and escalate requests from very important persons (VIP users), which comprise approximately 2% of the user population, as identified by the designated VIP flag in ServiceNow and detailed by the NETL approved priority service guideline.
- Prioritize and escalate service requests that are having a negative impact on data-taking for research projects that are actively taking data. If the service request occurs at a time when the project is not taking data, the response shall be in accordance with SLAs.
- Develop and maintain user help guides; and develop and conduct user training of all supported hardware, software, applications, and services.
- Develop and maintain instructions on the use of the video teleconference equipment and post instructions in NETL meeting rooms.
- Provide Customer outreach programs as directed by the Government which aim to educate and provide information to users on IT topics.
- Perform the IT tasks associated with user onboarding/offboarding, which includes but is not limited to, user account creation/disablement/reassignment; desktop/laptop/VoIP phone configuration, setup, and delivery; and IT equipment collection.

Meeting Room Support

The Contractor shall provide support for NETL's executive meeting rooms, general conference rooms, video teleconferencing rooms, conference centers, research visualization laboratories, the Morgantown Innovation Center, and the systems and services required to effectively utilize these venues. The requirements shall include but are not limited to:

- Use and maintain developed processes to schedule rooms; determine meeting requirements; coordinate and arrange conference rooms per end user requirements; manage conference room calendars; provide assistance to users; and document user requirements and provision services.
- Coordinate with local scheduling staff (i.e., receptionist), requestor, and/or requestor's support staff to resolve scheduling conflicts and equipment needs, as well as determine room configurations and users' technology requirements.
- Schedule video teleconference room sessions and ensure that video teleconference rooms and equipment meet requirements of session participants.
- Provide technical assistance with web conferencing tools, which includes but is not limited to Microsoft Teams and Cisco Webex.

Endpoint Support

The Contractor shall provide technical support for NETL's endpoints, which include but are not limited to desktops, laptops, tablets, VoIP phones, smartphones, print devices, and endpoint peripherals. The requirements shall include, but are not limited to:

- Provide support for the imaging, deployment, and maintenance of client systems (computers and laptops). Deployment includes delivering the client system to the customer's work area remotely and when onsite; configuring and connecting the client system; and testing the client system for functional operation.
- Manage and perform equipment relocation, installation, expansion, and connection/disconnection of computer systems hardware and peripheral devices including but not limited to surveying new installations and moving IT equipment as requested.
- Coordinate the shipping and receiving of IT equipment to facilitate the transit of GFE to remote employees.
- Provide integration and support for a variety of peripheral devices such as printers, scanners, external storage devices, A/V devices, data acquisition platforms, control platforms, and other accessories.
- Maintain and operate a central repository for providing, maintaining, and managing a "loaner pool" of common (not high-end/specialized) computing devices (laptops, thick client workstations, tablets, etc.).
- Manage spare/replacement parts for high-end/specialized research computing devices as directed by the Government.
- Provide the management, logistics, and technical support for wireless services, including mobile devices like iPhones and iPads; and working with service providers to resolve installation, performance and service disconnect issues in a timely manner as needed.
- Review usage invoices for wireless services and verify charges; coordinate the funding coverage of base and overrun costs by the using organizations; and provide recommendations on how to maximize funds.
- Manage NETL accounts for GETS, WPS, and TSP Programs, as well as maintain and operate a central repository for provisioning GETS and WPS services.
- Support major endpoint improvement projects, including but not limited to, annual workstation lifecycle replacements and operating system upgrades/migrations.
- Recognize the unique nature of research computing devices and perform all work on research computing devices (upgrades, repairs, patching, etc.) in such a manner as to not negatively impact the research either through the disablement of the computing device or loss of data. It is understood that this does not include specific direction from the Government to disable a computing device due to its potential risk to the IT environment.
- Provide troubleshooting and hardware repair support for NETL endpoints and peripherals.
- Provide on-site and remote repairs (when possible) for desktop computers, laptops, smartphones, tablets, printers, monitors, and other peripherals, consisting primarily of component replacement.
- Handle warranty support: determine if failed systems or components are under warranty; contact the appropriate manufacturer; obtain the replacement part(s); and return the defective system or component to the manufacturer in accordance with manufacturer's disposition instructions and coordinate with the Government.
- Assist with annual network printer lifecycle replacement, printer upgrades, and minor repairs.
- Provide technical support and pro-active maintenance for network printers including but not limited to clearing paper jams, installing maintenance kits, and installing fusers.
- Provide input into the NETL-Standard Hardware List for hardware (such as monitors, computers towers, and laptops).

3.3.6 *Performance Expectations/Inspection and Acceptance*

The performance expectations for the Client Delivery CLIN are summarized into performance objectives listed below followed by the performance expectation and the surveillance method. The performance expectation is the standard for which services will be accepted.

Performance Objective	Performance Expectation	Surveillance Method
The Contractor shall ensure efficient, effective, prompt, courteous, and timely Service Desk support.	>=93.5% of customers report on surveys a satisfactory or higher rating when dealing with Service Desk support services. >=64% of all service incidents are resolved during the first call. >=98% of all service requests are triaged, prioritized, and assigned appropriately. >=96.5% of all service requests and incidents are resolved and closed within the appropriate amount of time as determined by the ticket severity: • Priority 1: Immediate • Priority 2: 4 Business Hours • Priority 3: 1 Business Day • Priority 4: 3 Business Days • Priority 5: Scheduled with Customer	NETL shall assess the degree to which Service Desk support is efficient, effective, prompt, and courteous through customer surveys and validated customer complaints. NETL shall assess the degree to which the Service Desk support is timely through periodic audits of monthly reports and periodic audits of the incident tracking system.
The Contractor shall follow the NETL IT Incident Communication Plan during a Major IT Incident/Outage event.	The Contractor shall notify the government immediately (within 15 minutes) and provide hourly updates until the issue has been resolved.	NETL shall assess the communication response times to major incidents/outages of Infrastructure Operations Services through COR observations and review of SIR and Incident Reports.
The Contractor shall perform the IT tasks associated with user onboarding/offboarding, which includes but is not limited to, user account creation/ disablement/ reassignment; desktop/laptop/VoIP phone configuration, setup, and delivery; and IT equipment collection.	The Contractor shall ensure that all IT activities associated with onboarding/offboarding are completed as noted below– a minimum of 99% compliance and strive for 100% compliance. • New Employee Active Directory / LAN accounts are created and available to users on their start date as identified by the Personnel Tracking System (PTS) • New Employee IT equipment (laptop, desktop, Desk Phone, etc.) are setup and available in an employee's office or available onsite for pickup on	NETL shall assess the degree to which the onboarding/offboarding activities are performed is timely through COR observations, periodic audits of monthly reports and periodic audits of the incident tracking system.

	their start date as identified by PTS • New Employee IT equipment (laptop, desktop, Desk Phone, etc.) are setup and available to ship to remote employees within 3 business days of their start date as identified by PTS • Exiting Employee Active Directory / LAN and other resource accounts are made inactive within 1 business day of their end date as identified by PTS • Exiting Employee Active Directory / LAN and other resource accounts are made inactive within 1 business day of their end date for employee separation actions that are not entered into PTS • Exiting Employee IT equipment (laptop, desktop, Desk Phone, etc.) is accounted for prior to the employee's end date as identified by PTS • Exiting Employee IT equipment (laptop, desktop, Desk Phone, etc.) is accounted within 1 business day of their end date for employee separation actions that are not entered into PTS	
The Contractor shall provide smooth functioning meeting room support for meetings with external entities.	Since NETL needs a professional external face, the minimum requirement is 99% compliance while the Contractor needs to strive for 100% smooth functioning meetings with external entities.	NETL shall assess the compliance through Customer satisfaction/dissatisfaction feedback.
The Contractor shall perform all work on research equipment in such a manner that data is not lost/harmed due to Contractor's negligent interaction with the equipment.	As research data is somewhat irreplaceable and expensive to acquire, the minimum requirement is 99% compliance while the Contractor needs to strive for 100% "no harm" to research data.	NETL shall assess the degree to which interactions with research equipment are managed appropriately through review of the monthly activity reports, and periodic audits, and Customer satisfaction/dissatisfaction feedback.

3.3.7 Deliverables/Schedule

Monthly Activity Report – The Contractor shall provide a monthly report of the Client Delivery activities, including but not limited to:

- Initiatives Summary – current initiatives, status, etc.
- Applications and Services Status Monitoring Summary – uptime, outages, service interruption reports, problems, corrective actions, etc., for all IT services.
- Service Desk Summary – highlights of monthly activities and first Call resolution statistics, including the status of any open tickets that are not expected to be resolved quickly (or within the SLA time).
- Wireless Service usage and costs.
- Purchasing Support Summary – purchase requests submitted, upcoming purchases and purchases received.

Service Desk Surveys – The Contractor shall maintain an automatically-sent email survey to customers at agreed upon intervals, configuring the survey to be returned to the federal CLIN monitor. The Service Desk Survey contains 5 to 10 questions asking the customer to rate the support, response, resolution, etc.

Service Interruption Report (SIR) – The Contractor shall submit a SIR for every IT service outage or significant degradation within five days of the event. The SIR shall include detailed event information, findings, remediation activities, and lessons learned. (Typically, there are less than 25 of these a year.)

Quarterly Print Management Report – The Contractor shall provide a quarterly sortable and filterable list of imaging devices which includes device name, device location information, device model, device type, device functions, duty cycle, device status information (New, Legacy, Excessed), usage, and property tag number.

3.4 CLIN 00002 – Infrastructure

3.4.1 CLIN Type

This CLIN is firm-fixed price.

3.4.2 Place of Performance

For operations and maintenance actions requiring hands-on work or face-to-face, in-person Customer interaction, the place of performance for this CLIN is at NETL sites Albany, OR, Morgantown, WV, and Pittsburgh, PA.

3.4.3 Objectives

The primary objective of the infrastructure CLIN is to ensure that the whole suite of Infrastructure Services is fully performant, available, reliable, and secure to meet NETL mission requirements while minimizing operational impact on NETL.

3.4.4 Scope/Requirements

Infrastructure is a function within the Enterprise organization and encompasses all the infrastructure capabilities and services that support the Enterprise environment, as well as the common IT services shared across NETL for which Enterprise is responsible, which includes:

- Data Center
- Networks
- Telecommunications
- Client Services Engineering

The Contractor shall provide NETL with all supervision, personnel, tools, equipment, and services (excluding those items identified under the Government-furnished section of the contract) to satisfactorily perform the infrastructure services identified in this CLIN. It is expected that the Contractor shall perform in accordance with the specified SLAs.

Essential infrastructures Services are those services which are required to be available and operational 24 hours a day, 7 days a week, 365 days a year, even during site closings for weather. During NETL business operation hours, it is expected that the loss of Essential Infrastructure Services shall result in immediate (within 15 minutes) response times for remediation. At all other times, it is expected that the Contractor shall respond within 60 minutes and have staff on-site within 2 hours of initial contact to troubleshoot and resolve the service interruption or identified problem per Government direction.

3.4.4.1 General Requirements

The Contractor shall perform all work within this CLIN according to the requirements specified in General Contract Requirements section 2.0. In addition, the Contractor shall perform the general infrastructure activities across all infrastructure areas (Data Center, Networks, Telecommunications, and Client Services Engineering), which include:

- Perform all **preventive maintenance** activities within the Enterprise environment without negatively impacting the NETL user community in accordance with the Annual Preventative Maintenance Plan, where requirements shall include but are not limited to:
  - Create and submit an annual preventative maintenance plan and schedule.
  - Provide a list of planned activities no less than 3 days prior to the preventive maintenance date, after the annual preventive maintenance plan and schedule have been approved by the Government.
  - Apply hardware and software security/vulnerability patching to maintain supported versions and to meet security requirements. It is expected that patching is promoted from Development, to Test, to Production when capability exists to test in multiple environments.
  - Apply all patches which can be safely applied in accordance with NETL's SLAs, otherwise the Contractor shall document and register the risk if it is found that the patches are not applicable or would cause harm to the functionality of the application/system/network.
  - Apply patches and remediations when required by mandates, BODs, and government cybersecurity alerts and complete by the stated deadlines.
  - Coordinate all normal updates and remediations to research workstations—particularly for those attached to ICSs—with system owners to prevent harm to the research project. Care shall be taken to not impact a research project during data taking/creating.
  - Manage all research workstation emergency updates and remediations according to direction from the COR or the Technical Contracting Officer Representative (TCOR).

- The Contractor shall ensure knowledge management as described in *Governance [2.1]* under *General Contract Requirements [2.0]* and provide up-to-date **technical documentation and drawings** for Infrastructure services, systems, and networks; requirements shall include but are not limited to:
  - Create and maintain technical design documents, specifications, diagrams, and architecture artifacts for all infrastructure solutions. At a minimum, the artifacts shall include information which describes its business purpose, technical configuration, technical features and functions, network connectivity, integration with other systems and technical dependencies.
  - Create and maintain up-to-date floor plans and rack elevations drawings of each NETL data center.
  - Create and maintain accurate as-built documentation for all data center assets. At a minimum, documentation shall include system name, property number, operating system version, Internet Protocol address, age of unit, and hosted applications.
  - Create and maintain accurate as-built drawings and documentation for all Network and Telecommunication assets, as well as detailed Cable Plant diagrams.

  - Create and maintain accurate as-built documentation of all NETL's client standard operating environments (SOEs). At a minimum, documentation shall include information about the base operating system, custom configurations, and an inventory of standard applications installed.
  - Perform annual reviews of all technical documentation to ensure that they are up-to-date and relevant.

- The Contractor shall **continuously monitor** the health, security, availability, and performance of the Enterprise environment, using Government approved tools, to ensure proactive corrective actions are taken in response to issues, compromises, or degraded performance.

- The Contractor shall conduct any necessary **testing or validation** activities before and after the implementation of changes or deployment into the production Enterprise environment to minimize IT Service disruptions. In addition, the Contractor shall perform regular proactive testing and validation of IT applications and services to ensure that they are functioning and performing as expected from the Customer's perspective.

- The Contractor shall conduct **performance management** to ensure performance optimizations of Enterprise applications, services, systems, and networks while maintaining efficient and effective operations to maximize user productivity.

- The Contractor shall provide **resource utilization and capacity planning** support and shall be responsible for providing recommendations for equipment and service replacement, upgrade, or enhancement to prevent the delivery of services from falling below acceptable levels as identified through utilization trends.

- **Disaster Recovery Plan (DRP)** – The Contractor shall develop, maintain, and test each calendar year a disaster recovery plan for all NETL applications, systems, networks, and services which is well-structured and easily understood, to aid NETL in the recovery of business operations as quickly and effectively as possible from an unforeseen disaster event. Additional requirements include but are not limited to:
  - The DRP shall be completed within the first 12 months of the Contract – fully tested.
  - Perform annual DRP testing to ensure that it can be implemented in real disaster situations and help staff understand how it is to be executed. Scheduling of the testing shall be approved by the Government to avoid impacting any Government functions.
  - Present DRP and test results to the Government for feedback and acceptance.
  - Maintain an up-to-date plan which reflects changes in the IT environment and evolving technologies implemented at NETL.
  - The recovery procedures shall include step-by-step technical instructions for restoring applications, services, networks, and systems.
  - The DRP documentation shall be stored in a secure offsite location as directed by the COR/TCOR.

- The Contractor shall **support NETL construction and renovation projects** at Albany, Morgantown, and Pittsburgh, where requirements shall include but are not limited to:
  - The Contractor shall support the design activities which include:
    - Develop design requirements based on functional requirements.
    - Review drawings and specification packages (15%, 50%, 95%, 100%) and provide written comments.
    - Review product submittals and provide written comments.
    - Develop minimum acceptance test requirements.
  - The Contractor shall support construction activities which include:
    - Participate in weekly construction coordination meetings.
    - Perform construction site inspections.
    - Observe system installation, setup, and testing; and provide written comments of the findings.
    - Observe and Document acceptance testing and provide written comments of the findings.

        - Review certification test results and provide written comments of the findings.
        - Review project documentation for completeness and accuracy and update NETL documentation as required.
        - Attend training on the new systems.

- The Contractor shall conduct **continuous improvement** activities, where requirements shall include but are not limited to:
    - Proactively recommend changes and/or enhancements to the Enterprise environment to provide better efficiency, productivity, stability, and/or cost savings within the larger scope of each project's requirements.
    - Provide continuous assessment and optimization to deliver operational recommendations to NETL for the improvement of IT services.
    - Evaluate metrics and usage and provide NETL with data on potential areas which could be improved, as well as ideas of how those improvements could be implemented.

3.4.4.2 Data Center Requirements

The Contractor shall deliver data center co-location hosting services and both on-premises and cloud Infrastructure-as-a-Service (IaaS) to support NETL applications and services. In addition, the Contractor shall manage core data center services including directory services, data storage services, external file transfer services, backup and recovery services, and enterprise monitoring services. Data Center Hosting Services, Directory Services, and Data Storage Services are Essential Infrastructure Services.

- The **Data Center Hosting Services** requirements shall include but are not limited to:
    - Support and manage all NETL data center hosting infrastructures and facilities including NETL private cloud environments, public cloud environments, and future computing infrastructures.
    - Ensure that data center servers, storage systems, and services are functional, secure, accessible, and usable 24 hours a day, 7 days a week, 365 days a year, except for planned, pre-approved outages for preventative maintenance, scheduled outages, or other related activities. The Contractor shall maintain availability of all Data Center services, striving for 100% up-time and no less than 99.5% up-time.
    - Ensure that all data center assets are fully monitored at all times using Government approved tools, with automatic notifications configured to immediately alert staff of problems or failures. Upon detection of problems or failures, the Contractor shall perform immediate remedial actions to stabilize or restore the associated IT services and notify Federal designee of the problems or failures in accordance with the NETL incident response procedure.
    - Maintain data center facilities in accordance with NETL's data center management policies and procedures.
    - Coordinate and support on-premises data center cleaning activities.
    - Provide technical expertise to define requirements for facility support services in the data center, which include HVAC, fire suppression, power, lighting, and physical access.
    - Perform installation and setup of data center equipment including servers, appliances, storage systems, network devices, as well as establishing physical network and power connectivity. This also includes working with NETL customers to perform work as part of providing data center co-location services.
    - Coordinate and support the migration and moving of data center assets to other platforms, other data centers, and/or cloud instances and ensure compatibility, integrability, connectivity, and security of the systems.
    - Maintain NETL's server virtualization environment to ensure availability, reliability, capacity, performance, and security. This includes but is not limited to the management of physical servers and storage, hypervisors, virtual machines, containers, virtual networks, and virtual storage.

  - Maintain NETL's enterprise storage systems and networks to ensure availability, reliability, capacity, performance, and security. This includes but is not limited to the installation, configuration, provisioning, troubleshooting, and repair.
  - Be responsible for the activities associated with the investigation of new operating systems, installation techniques and options, the maintenance and update options for new and existing servers, and the configuration of the many different components of the server's operating system to provide for reliable and stable integration.
  - Design, develop, and maintain standardized server images for deployment purposes. This includes but is not limited to activities associated with the creation and maintenance of preconfigured server baseline images to facilitate rapid deployment and restoration.
  - Apply patches and remediations to these systems when required by cybersecurity mandates, BODs, and government cybersecurity alerts and ensure full compliance with the requirements and stated deadlines.
  - Develop, implement, and maintain a viable server protection scheme which protects the server and network against malicious code (viruses, trojans, spyware, malware, etc.), as well as unauthorized access to the system or its components.
  - Be responsible for controlling access to the data centers and all equipment therein, thus being responsible for tracking who has access to or enters the data centers, and for implementing a monitoring, tracking and approval process for incoming and outgoing equipment/servers from the data centers.

- **Core Data Center Services** requirements shall include but are not limited to:
  - Maintain NETL's enterprise monitoring tools used to monitor the health status and availability of all Enterprise environments and to support IT event management.
  - Document and perform server backups to provide for system restoration, file and database recovery, and disaster recovery. The Contractor shall operate and maintain the backup and restore processes without negatively impacting the NETL user community and shall be able to restore data for the previous 30 days and fulfill user restore requests within 3 days.
  - Facilitate off-site tape/on-premises backup/cloud backup data storage to support data restoration and disaster recovery operations.
  - Be responsible for software license server management within the enterprise environment.
  - Provide access management both to the physical components and to the digital environment to prevent unauthorized access in accordance with approved NETL processes and procedures.
  - Be responsible for account management, authentication, multi-factor authentication (MFA), public key infrastructure (PKI), and ensure that there is no unauthorized access to NETL systems and networks.
  - Ensure that all domain administrative accounts and all elevated privileged accounts have government approval prior to creation, where user accounts and permissions are granted and created using the NETL user account procedures and processes; in addition, annual audits of these accounts shall be conducted to ensure validity.
  - Maintain user groups, roles, and specific user accounts for applications.
  - Be responsible for directory services which include but are not limited to the management of active directory domains, directory objects (Users, Groups, Computers, and Containers/Organizational Units), group policies, federation services and Domain Name Services (DNS).
  - Operate and maintain the NETL directory services environment in accordance with NETL approved security hardening procedures.

3.4.4.3 Network Requirements

The Contractor shall provide management services for Network Security and Control Services, Internal Network Management Services, External Network Management Services and Core Network Services which support on-premises connectivity and connectivity to Enterprise cloud PaaS and SaaS application services. All of these services are Essential Infrastructure Services.

- **Network Security & Control** services include Firewall Services, Network Access Control, Network Micro-segmentation, Intrusion Prevention and Detection Services (IPS/IDP) and Zero Trust Architecture (ZTA). The requirements shall include but are not limited to:
  - Maintain Firewall Services ensuring availability, reliability, performance, and security.
  - Add, delete, and change firewall rulesets upon request, where rulesets shall be configured as restrictive as possible using next generation firewall feature sets such as application-based or user-id based rulesets.
  - Work with external entities to add, delete, or change rulesets that are not directly controlled by NETL.
  - Maintain Network Access Control (NAC) services for device authentication when connecting into the network, where authentication shall be configured as restrictive as possible to prevent unauthorized access to the network and all client facing network devices shall be configured with NAC services.
  - Maintain IPS/IDS ensuring availability, reliability, performance, and security; and ensure that the required network traffic flow is monitored.
  - Add, delete, and change Switched Port Analyzer (SPAN)/Monitor sessions.
  - Implement and maintain cable paths to enable traffic flows over the IDS/IPS devices.
  - Work with the cybersecurity team to ensure they are receiving the required data logs for analysis.
  - Support the effort to transition to a network architecture based on ZTA cybersecurity principles, in accordance with government mandates (Executive order on "Improving the Nation's Cybersecurity"), which includes design and implementation work. In addition, the Contractor shall provide network micro-segmentation management services in accordance with best practices.
  - Be responsible for controlling and tracking access to network assets and work closely with other teams to participate in NETL's identity and access management process to prevent unauthorized access to NETL's networks.

- **Internal Network Management** services include Cable Management, Network Hardware Management, Network Switching & VLANs, Network Routing, Network Virtualization (cloud only) and Wireless Network (cloud managed service). The requirements shall include but are not limited to:
  - Perform network cable management; this includes terminating and testing network station cabling (cable installed by others) and supporting projects to replace aging cable infrastructure across the NETL campus (includes design review, work inspections, and technical documentation).
  - Maintain all network hardware, which includes installations and deployments, troubleshooting and repairs, and device lifecycle management.
  - Provide managed LAN services. This support shall include but not be limited to addition and maintenance of infrastructure, network configuration services, network monitoring and management, and incident management and response.
  - Perform VLAN management, where VLANs shall be configured to be as restrictive as possible to maximize security.
  - Perform management of Network Switching to add, remove, and change switch design, implementation, and configurations.
  - Perform management of Network Routing to add, remove, and change routing design, implementation, and configurations.
  - Provide managed Wireless Local Area Network (WLAN) services, for internet access across all NETL locations, which includes maintaining and monitoring the wireless network infrastructure using a cloud-managed solution.
  - Provide management and configuration of Linux-based firewall solutions for research networks to provide isolation and protection of research systems.
  - Provide network support as needed for research projects (e.g., the use of Precision Time Protocol (PTP) needed for one research project). Recognizing that researchers are not IT

specialists, the Contractor shall assist researchers in any communications-type troubleshooting between devices, particularly those that are networked.

- **External Network Management** services include Network Routing, Demilitarized Zone Network (DMZ) networks, Internet and TIC services, Cloud Networks, and Virtual Private Network (VPN). The requirements shall include but are not limited to:
  - Maintain Virtual Private Network (VPN) services which support GFE endpoints. The Contractor shall support and enforce multi-factor authentication, provide client software to be installed on endpoints which is compatible with NETL endpoints, and maintain a multi-site high availability and redundant architecture.
  - Provide managed wide area network (WAN) services, which includes but is not limited to addition and maintenance of infrastructure, network configuration services, network monitoring and management, and incident management and response.
  - Perform managed network routing to optimize network performance, while ensuring a secure, reliable, and robust WAN network.
  - Perform network circuit management, which includes monitoring, troubleshooting, and repairing WAN connectivity issues, where remediation activities could involve initiating and managing vendor's technical support services.
  - Maintain Internet and TIC services and work with other DOE entities to maintain and optimize traffic to/from DOE TIC services and the Internet.
  - Perform DMZ network management, which includes adding, removing, and changing network configuration to maintain secure DMZ networks in accordance with best practices, where DMZ networks shall be configured as restrictive as possible.
  - Perform cloud network management. The Contractor shall design, implement, and maintain network connectivity to Cloud Service Providers (CSP) and design, implement and maintain virtual networks within Cloud IaaS solutions.

- **Core Network Services** include Domain Name Services (DNS), Dynamic Host Configuration Protocol (DHCP), Network Time Protocol (NTP) and IP (Internet Protocol) Address Management. The requirements shall include but are not limited to:
  - Maintain IP Address Management (IPAM) services, which includes the management of both IPv4 and IPv6 address schemes. IP assignments shall be planned and assigned logically to minimize network complexity and to ensure expandability for future growth. The Contractor shall support the effort to transition all IT assets from IPv4 to IPv6 address schemes in accordance with government mandates.
  - Maintain NTP services, which includes configuration of NTP synchronization to ensure that all NETL systems and devices have accurate and correct time.
  - Maintain DNS, ensuring functionality, availability, reliability, performance, and security.
  - Maintain DHCP services, ensuring functionality, availability, reliability, performance, and security.

3.4.4.4 Telecommunications Requirements

The Contractor shall provide management services for Telephony/Voice over IP (VoIP) Services, Audio/Video (A/V) Services, and the Radio Frequency Program. The Radio Frequency Program is an Essential Infrastructure Service.

- The Contractor shall manage **Telephony/VoIP Services** where requirements shall include but are not limited to:
  - Maintain NETL's Unified Communication infrastructure, in accordance with current technology standards and all applicable Federal and Department regulations.
  - Maintain NETL's Unified Communication platform and applications, which include installation, configuration, and troubleshooting and repairing issues.
  - Provide continuous (24 hours/day, 7 days/week) application performance monitoring, incident detection, and problem resolution.
  - Coordinate and execute authorized Unified Communications services moves, adds, and

changes.
  - Manage the NETL voice cable infrastructure maintaining as-built records with annual updates.
  - Audit Unified Communications accounts annually to ensure service assignments are current, accurate and comply with NETL requirements, best practices, and applicable regulations.
  - Terminate copper cable (Cat 3, Cat 5) installed by NETL.
  - Provision analog services to endpoints.
  - Coordinate site access for service provider repairs and equipment upgrades.
  - Develop technical requirements for the acquisition of new telecommunication services or modification to existing services.
  - Coordinate authorized changes to telecommunications services, which includes installation, upgrades, and disconnects.
  - Coordinate the renewal of existing telecommunications services and the purchase of new telecommunications services through DOE HQ, Government agencies such as General Services Administration (GSA) and commercial vendors.
  - Manage NETL accounts for DOE HQ telecommunications services, including reviewing monthly invoices for reasonableness, maintaining call detail and invoice records per National Archive and Records Administration (NARA) requirements, and providing notification when charges exceed established criteria.
  - Manage NETL accounts for web collaboration, audio conferencing, and commercial television (i.e., cable, satellite, fiber, etc.) services.

- The Contractor shall manage **A/V Services** for standard conference rooms and VTC rooms, where requirements shall include but are not limited to:
  - Provide Tier 2 support for standard conference rooms and VTC rooms to include problem identification, system troubleshooting and repair, maintaining spare parts, making repairs, escorting service providers, and coordinating equipment repairs.
  - Provide subject matter expertise to develop requirements for VTC system upgrades and implement the authorized upgrades.
  - Provide Tier 2 support for NETL's displays (for commercial TV, NETL information, etc.) at Albany, Morgantown, and Pittsburgh.
  - Work with Meeting Room Support technicians *[CLIN 00001]* to provide support for meeting room setups.
  - Support web collaboration meetings as an alternative to in-person meetings or program reviews.
  - Provide end user training on the Audio/Visual and collaboration applications in NETL's VTC rooms.

- The Contractor shall manage, operate, and maintain NETL's Conference Center and Executive Meeting Room A/V systems, where requirements include but are not limited to:
  - Configure and operate A/V systems in accordance with current technology standards, best practices, and all applicable Federal and Department regulations.
  - Qualified staff shall configure, operate, and repair A/V systems.
  - Conference Centers and Executive Meeting Rooms have appropriate Contractor provided support contracts to ensure performance issues and security vulnerabilities are addressed within specified SLAs.
  - Conference Center and Executive Meeting Room A/V systems shall have high availability during core business hours with failed systems replaced/repaired within 48-hours.
  - Develop system requirements from NETL functional requirements.
  - Develop "customized" requirements for NETL sponsored events.
  - Evaluate performance issues including the review of signal flow diagrams, audio system programming and control system programming.
  - Provide A/V expertise to evaluate design submittals for compliance with functional

requirements.
  - Deliver end user training on A/V and collaboration applications in NETL's executive conference rooms, conference centers, and the Morgantown Innovation Center.
  - Use standard processes to setup meetings and evaluate room performance.
  - Ensure that A/V systems are available and configured per the NETL meeting requirement.
  - Perform A/V repairs, upgrades and security patching according to the specified SLAs.
  - Ensure A/V systems are fully tested prior to returning the system to service when performing A/V system repairs, upgrades and security patching.
  - Address issues while minimizing the impact to meetings.
  - NETL's Conference Center and Executive Meeting Room A/V systems are described below.

- The Contractor shall manage, operate, and maintain NETL's research Visualization Laboratories (high-end state-of-the-art technology, augmented/virtual reality systems, etc.), where requirements include but are not limited to:
  - Provide qualified Tier 2 and Tier 3 support for research visualization laboratories to include problem identification, system troubleshooting and repair, maintaining spare parts, making repairs, escorting service providers, and coordinating equipment repairs.
  - Provide subject matter expertise to develop requirements for collaboration system upgrades and implement the authorized upgrades in accordance with current technology standards, best practices, and all applicable Federal and Department regulations.
  - Develop system requirements from NETL functional requirements.
  - Develop "customized" requirements for NETL sponsored events.
  - Evaluate performance issues including the review of signal flow diagrams, audio system programming and control system programming.
  - Provide A/V expertise to evaluate design submittals for compliance with functional requirements.
  - Deliver end user training on A/V and collaboration applications in NETL's research visualization laboratories.
  - Use standard processes to setup meetings and evaluate room performance.
  - Ensure that A/V systems are available and configured per the NETL meeting requirement.
  - Perform A/V repairs, upgrades and security patching according to the specified SLAs.
  - Ensure A/V systems are fully tested prior to returning the system to service when performing A/V system repairs, upgrades and security patching.
  - Address issues while minimizing the impact to meetings and room usage.

- The Contractor shall manage NETL's **Radio Frequency Program**, where requirements shall include but are not limited to:
  - Maintain NETL's LMR infrastructure in accordance with current technology standards and all applicable Federal and Department regulations.
  - Manage NETL's radio frequency assignments – ensure radio frequency authorizations are current (not expired), accurate, and address NETL's radio frequency communication requirements, including reviewing requests for new radio frequency assignments, evaluating radio frequency usage, and providing recommendations to add, delete and modify radio frequency authorizations.
  - Develop requirements for comprehensive maintenance contracts covering LMR systems including mobiles, base stations, and repeaters.
  - Manage the NETL radio frequency systems maintaining accurate inventories and as-built drawings with annual updates.
  - Evaluate licensing requirements for new equipment proposed for use at NETL facilities.
  - Provide management and problem resolution for NETL's LMR communication systems to include problem identification, system troubleshooting and repair,

    - maintaining spare parts, coordinating service calls, escorting service providers, and coordinating equipment repairs.
    - Maintain Subject Matter Expertise (SME) to ensure staff understand LMR configuration, operation, and programming.
    - Review requests by NETL staff to utilize radio frequency products in support of NETL projects.

3.4.4.5 Client Services Engineering Requirements

The Contractor shall provide management services for NETL's Standard Operating Environment, Client Software/Applications, Endpoint Management Services, Core Client Services, Virtual Desktop Infrastructure (VDI) services, Research Endpoint Engineering Services, Instrumented Control System (ICS) Support, and Research Cloud Support. Citrix Remote Desktop environment is an Essential Infrastructure Operations Service.

- The Contractor shall manage **NETL's Standard Operating Environment** where requirements shall include but are not limited to:
    - Develop and maintain secure, reliable, networked client systems at NETL for a variety of computing systems (workstations, laptops, data acquisition platforms, control platforms, and mobile computers) and peripherals (printers, scanners, external storage devices, audio/video devices, data acquisition platforms, control platforms, and other accessories) through the integration of computing hardware, client operating systems, network operating systems, and application software in compliance with relevant mandated policy regulations.
    - Be responsible for the activities associated with the investigation of new operating systems, installation techniques and options, the maintenance and update options for new and existing operating systems, and the configuration of the many different components of the client system's operating system to provide for reliable and stable integration of such in the NETL IT environment.
    - Design, develop, and maintain standardized client images for deployment purposes. This includes but is not limited to activities associated with the creation and maintenance of preconfigured workstation "images" to facilitate the rapid deployment of new equipment and the rapid restoration of existing equipment.

- The Contractor shall manage **Client Software / Applications** where requirements shall include but are not limited to:
    - Develop, test, maintain and deploy software packages for distribution to user endpoints, manual or automated deployment of software packages to endpoints and troubleshooting and resolving issues.

- The Contractor shall provide **Endpoint Management** services where requirements shall include but are not limited to:
    - Maintain NETL's endpoint management tools ensuring availability, reliability, performance, security, and proper configuration. The Contractor shall leverage these tools to increase efficiencies and effectiveness in endpoint management through automations and standardizations.
    - Develop, implement, and maintain a viable client system protection scheme which protects the client system and network against malicious code (viruses, trojans, spyware, malware, etc.), hard drive encryption, application whitelisting and unauthorized access to the system or its components (implementation of client system security policies and client firewalls).
    - Monitor, configure, and operate the mobile device management (MDM) solution deployed at NETL. The Contractor shall support NETL mobile device customers,

responding to new service requests, mobile device issues, tracking service requests and terminations, and MDM service issues.

- The Contractor shall manage **Core Client Services** where requirements shall include but are not limited to:
    - Manage services, servers, and infrastructure in support of file and print services.
    - Manage the Microsoft Office 365 cloud-based SaaS solution for business operations, which includes email, file storage, collaboration tools and Microsoft Office productivity tools.
    - Manage email encryption services for email clients and smartphones.
    - Provide support for smart cards and related digital certificates that are used as part of NETL's MFA solution.
    - Maintain and operate research networks' remote capabilities, including Remote Desk Protocol (RDP) and an NETL-created remote connection application.

- The Contractor shall manage **Virtual Desktop Infrastructure (VDI**) services where requirements include but are not limited to:
    - Maintain and operate Admin LAN's Citrix XenApp environment, including but not limited to installation, configuration and maintenance of the Citrix platform, user profile management, virtual desktop and application management, database management, access management and related system/user policies.
    - Maintain and operate NETL's Virtual Enterprise Environment (VEE).
    - Maintain and operate Research LAN's Citrix XenDesktop Environment.
    - Maintain and operate cloud based VDI solutions.

- The Contractor shall provide **Research Endpoint Engineering Services** where requirements shall include but are not limited to:
    - Provide research IT endpoint design services to the in-house research community. These design services are focused on understanding the requirements of the research customer and helping them find an IT endpoint (computer, printer, etc.) that fulfills their unique research requirements.
    - Provide research IT installation/setup services. The installation/setup services are meant to be a follow-up to the IT endpoint design services to the in-house research community such that once the IT endpoint has arrived at NETL, the Contractor helps the research customer make the endpoint functional. These services are primarily focused on setting up an endpoint, installing/updating the operating system (OS), installing software/applications, and connecting the endpoint to a network; it is not meant to include software configuration or extensive effort.
    - Install unique software per user request; however, the responsibility for configuration of that unique software falls on the user. (The Contractor may provide configuration assistance in some limited cases.) Maintenance/upgrade responsibilities are to be clearly defined for each unique software installation as it may vary according to the IT-capabilities of the user.
    - Assist researchers in resolving any issue that appears to be IT-related (as researchers are not typically IT specialists).
    - Provide the skills to support the technology used by the in-house research community. Due to the nature of research and evolving technology, the Contractor shall be responsible for acquiring new technical skills as directed by the Government in support of in-house research.
    - Manage centralized knowledge of research ICSs for use in data calls and cyber/upgrade decisions, including System Owner, Research Project name, physical and network locations, Linux-based firewall solution usage/configuration, other associated

endpoints, OS, and ICS-specific software with its limitations.

- Develop, implement, and maintain viable client system protection schemes specifically tailored to the ICS environment which protect the client system and network against malicious code (viruses, trojans, spyware, malware, etc.), hard drive encryption, application whitelisting and unauthorized access to the system or its components (implementation of client system security policies and client firewalls) while not negatively impacting the ability to do research.

3.4.5 Performance Expectations/Inspection and Acceptance

The performance expectations for the Enterprise Infrastructure CLIN are summarized into performance objectives listed below followed by the performance expectation and the surveillance method. The performance expectation is the standard for which services will be accepted.

Performance Objective	Performance Expectation	Surveillance Method
The Contractor shall ensure that all Enterprise Infrastructure services are available, functional, secure, accessible, and usable 24 hours a day, 7 days a week, 365 days a year, except for planned, pre-approved outages for preventative maintenance, scheduled outages, or other related activities.	The Contractor shall maintain a minimum of 99.5% uptime, measured monthly, and strive for 100% availability.	NETL shall assess the availability of Enterprise Infrastructure services through COR observations and review of Monthly Activity Reports (MARs), Service Interruption Reports (SIRs), Incident Reports, and Availability Reports.
The Contractor shall address major Enterprise incidents/outages within established NETL SLAs and shall provide issue resolution, including identifying issues, troubleshooting, and repairing. The Contractor shall strive to restore normal operations as soon as possible.	During business hours: • Response time for remediation = Immediate (within 15 minutes) • All outages resulting in a service impact shall have an associated Service Interruption Report within 5 business days. During non-business hours: • Response time for remediation < 1 hour • The Contractor shall have staff on-site if required for remediation, within 2 hours of the initial contact. • All of outages resulting in a service impact shall have an associated Service Interruption Report within 5 business days.	NETL shall assess the response times to remediate major incidents/outages of Enterprise Infrastructure services through COR observations and review of Monthly Activity Reports (MAR), SIR, Incident Reports, and Availability Reports.

The Contractor shall follow the NETL IT Incident Communication Plan during a Major Enterprise Incident/Outage event.	During business hours: • The Contractor shall notify the government immediately (within 15 minutes) and provide hourly updates until the issue has been resolved. During non-business hours: • The Contractor shall notify the government in less than 1 hour and provide hourly updates until the issue has been resolved.	NETL shall assess the communication response times to major incidents/outages of Enterprise Infrastructure services through COR observations and review of SIR and Incident Reports.
The Contractor shall implement Enterprise Infrastructure changes in accordance with NETL's Change Management process.	All changes to the Enterprise Infrastructure shall be approved by the CAB before change implementation – 100% compliance.	NETL shall assess the degree to which Change Management is performed through COR observations and review of Monthly Activity Reports (MAR), Service Interruption Reports (SIR), Incident Reports, and Availability Reports.
The Enterprise environment shall be scanned, patched, and updated per agreed upon schedule, without negatively impacting the NETL user community.	The Contractor shall complete the patching activities within agreed upon Preventative Maintenance Schedules - 100% compliance. The Contractor shall patch the infrastructure environments according to schedule - 100% compliance. • Data Center systems and services are scanned, patched and updated within the **two weeks** of patch release, unless superseded by government mandates. • Network devices, telecommunication devices/services, audio/visual devices and radio frequency systems are running vendor/ manufacturer supported operating systems with appropriate patching to mitigate known vulnerabilities, within **60 days** of patch release, unless superseded by government mandates. • Endpoints are scanned, patched and updated within **30 days** of patch release,	NETL shall assess the degree to which vulnerability remediation activities is performed on-time and without service interruption through COR observations and review of the MAR, Vulnerability Scans, SIR, Incident Reports and Availability Reports.

	unless superseded by government mandates.	
The Contractor shall ensure that there is no unauthorized access to Enterprise applications, systems, and networks.	The Contractor shall ensure that only authorized users and devices are allowed access to Enterprise applications, systems, and networks at all times – 100% compliance. The Contractor shall remove or disable retired/expired accounts within 30 days within the Enterprise environment – 100% compliance. The Contractor shall enforce government mandated MFA, where all exceptions must be documented and approved by the government – 100% compliance.	NETL shall assess the degree to which unauthorized access to Enterprise applications, systems and networks is enforced through COR observations, quarterly stale account audits, MFA compliance tracking, and cybersecurity incident reports.
The Contractor shall ensure that NETL data center access is monitored and controlled at all times; only authorized users can access NETL on-premises data centers, and any unauthorized access is eliminated as soon as possible after identification.	No unauthorized data center access is permitted at all times – 100% compliance.	NETL shall assess data center access compliance through COR observations and review of data center access logs and reports.
The Contractor shall ensure functional, secure, robust, and reliable data recovery services for all Enterprise applications, systems and networks.	The Contractor shall be able to restore data for no less than the previous 30 days, fulfilling user restore requests within 3 days. The Contractor shall be able to restore enterprise database service for no less than the previous 30 days, fulfilling restore requests within 36 hours. Backup media shall be transported off-site on a weekly basis and stored in a fireproof container for a minimum of 5 weeks – 100% compliance. The Contractor shall ensure that there is, at minimum, a weekly backup copy stored at another location to support Disaster Recovery operations – 100% compliance.	NETL shall assess the degree to which the data services backups are functional and secure through COR observation, random audits and backup reports. NETL shall assess the degree to which restore requests are fulfilled successfully within the required timeframe through random audits, incident reports, service desk surveys and customer feedback.

The Contractor shall develop, maintain, and test each calendar year a disaster recovery plan for all NETL applications, systems, networks, and services that is well-structured and easily understood, to aid NETL in the recovery of business operations as quickly and effectively as possible from an unforeseen disaster event.	The Contractor shall complete a fully tested DRP within the first twelve months of the Contract. The Contractor shall submit an updated DRP at the end of each calendar year. The Contractor shall perform and formally document annual DRP rehearsals to validate the recovery procedures at the end of each calendar year.	NETL shall assess the degree to which the DRP deliverables are completed through COR observation, random audits, review of the DRP rehearsal documentation, and review of the completed DRP.
The Contractor shall ensure software compliance and license management as well as warranty tracking such that all production hardware and software is always within the original manufacturer's equipment warranty or under vendor support maintenance agreement, as well as recording and tracking license distributions to ensure compliance.	The Contractor shall ensure that all Enterprise Infrastructure hardware and software is always within the original manufacturer's equipment warranty or under vendor support maintenance agreement – 100% compliance. The Contractor shall ensure that license distributions do not exceed the number owned by NETL – 100% compliance. The Contractor shall notify the government of hardware or software that will go EOL and EOS at least 24 months before the EOL or EOS date, as part of the IT asset lifecycle management process - 100% compliance.	NETL shall assess the degree of success in the management of software and hardware maintenance is through COR observations, random audits of license utilization, license reports, maintenance contract reports, MARs, and Biannual Improvements Plan.
The Contractor shall ensure knowledge management, including up-to-date documentation and drawings for Enterprise Infrastructure.	Creation or updates to Enterprise Infrastructure documentation will be made available no later than 5 days following a release to production – 100% compliance.	NETL shall assess the degree to which technical documentation is maintained through inspection and review of the technical documentation artifacts and random audits.
The Contractor shall continuously monitor the health, security, availability, and performance of all Enterprise applications, systems, and networks. The Contractor shall ensure continuous logging of all Enterprise applications, systems, and networks.	The Contractor shall ensure that all Enterprise applications, systems and networks are monitored at all times via NETL's enterprise monitoring tool - 100% compliance. The Contractor shall ensure that all Enterprise application, system, and network logs are captured and made available on a continuous basis - 100% compliance.	NETL shall assess the degree to which applications, systems and networks are monitored through COR observations, random audits and review of the enterprise monitoring reports and dashboards. NETL shall assess the degree to which logs are made available through COR observation, inspection of logs and random audits.

The Contractor shall perform all preventive maintenance activities within the IT environment without negatively impacting the NETL user community in accordance with the Annual Preventative Maintenance Plan.	The Contractor shall submit an Annual Preventative Maintenance Plan to the government for review and approval 60 days before the start of a new calendar year - 100% compliance. The Contractor shall provide a list of planned activities no less than 3 days prior to the preventive maintenance date - 100% compliance.	NETL shall assess the degree to which the plans are submitted on-time through COR observation and review of the preventative maintenance schedule and plans.
The Contractor shall conduct performance management to ensure performance optimizations of Enterprise systems and networks while maintaining efficient and effective operations to ensure user productivity.	The Contractor shall maintain a minimum of acceptable levels of performance 99.5% of the time, and strive for 100%, where acceptable levels means that services are usable and does not impact user productivity.	NETL shall assess the degree to which performance of Enterprise systems and networks are maintained at an acceptable level through COR observation and review of monthly activity reports, service interruption reports, incident reports, availability reports, performance reports and the Semiannual Improvement Plan.
The Contractor shall provide resource utilization and capacity planning support and shall be responsible for providing recommendations for equipment and service replacement, upgrade, or enhancement to prevent the delivery of services from falling below acceptable levels as identified through utilization trends.	The Contractor shall maintain a minimum of acceptable levels of capacity 99.5% of the time, and strive for 100%, where acceptable levels means that services are usable and does not impact user productivity.	NETL shall assess the degree to which capacity of Enterprise systems and networks are maintained at an acceptable level through COR observation and review of monthly activity reports, service interruption reports, incident reports, availability reports, performance reports and the Semiannual Improvement Plan.
The Contractor shall ensure on-time and appropriate Service Purchasing support.	100% of software maintenance renewals are entered into the purchasing system on-time. 100% of the purchase requests are entered into the purchasing system within 2 weeks of submission. Marketing surveys are appropriate for the technical requirements and conducted within 1 month of request. Input for invoice/bill review is correct 100% of the time.	NETL shall assess the degree to which purchasing support is on-time and appropriate through review of the procurement records and Monthly Activity Reports.

3.4.6 Deliverables/Schedule

Disaster Recovery Plan (DRP) – The Contractor shall develop, maintain, and test each calendar year a disaster recovery plan for all NETL applications, systems, networks, and services which is well-structured and easily understood, to aid NETL in the recovery of business operations as quickly and effectively as possible from an unforeseen disaster event. Additional requirements include but are not limited to:

- A DRP shall be completed within the first nine months of the Contract – fully tested.
- Perform annual DRP testing to ensure that it can be implemented in real disaster situations and help staff understand how it is to be executed.
- Maintain an up-to-date plan which reflects changes in the IT environment and evolving technologies implemented at NETL.
- The recovery procedures shall include step-by-step technical instructions for restoring applications, services, networks, and systems.
- The DRP documentation shall be stored in a secure offsite location (which could include cloud).

Annual Preventative Maintenance Plan and Schedule – The Contractor shall provide a recommended annual preventative maintenance plan and schedule at the start of each new contract year, developed, and implemented in a manner consistent with industry standards and guidelines and manufacturer-recommended maintenance schedules.

As-Built Documentation – The Contractor shall provide documentation for applications within five days of the application being released into the IT production environment.

Monthly Activity Report (MAR) – The Contractor shall provide a monthly report of the infrastructure activities including but not limited to:

- Initiatives Summary – current infrastructure initiatives, status, etc.
- Applications and Services Status Monitoring Summary – uptime, outages, service interruption reports, problems, corrective actions, etc., for all infrastructure services.
- Purchasing Support Summary – purchase requests submitted, upcoming purchases and purchases received.
- Data Center resource utilization reports (e.g., virtual resources, storage, etc.)
- EOL/EOS report of all Enterprise Hardware and Software assets.

Quarterly License Utilization Reports – The Contractor shall provide a quarterly license utilization report for all Infrastructure services, to support planning activities and to track compliance. The report shall include but not be limited to Cisco Unified Communications (UC), Cisco VPN, Cisco ISE, Cisco Meraki, VMware, Microsoft and Citrix Licenses.

Service Interruption Report (SIR) – The Contractor shall submit an SIR for every IT service outage or significant degradation within five days of the event. The SIR shall include detailed event information, findings, remediation activities, and lessons learned. (Typically, there are less than 10 of these a year.)

Annual Audit Report for Administrative/Privileged Accounts – The Contractor shall submit a report that documents the full list of administrative or privileged accounts which identifies valid accounts and accounts which have been disabled/removed because they are no longer valid; the report should provide a description of why the account is valid and what it is used for.

Semiannual Improvements Plan for Continuous Improvements

- Software License Utilization
- Hardware Inventory Status
- Software & Hardware Lifecycle Status Report
- IT Asset and Technology Refresh Plans
- Capacity Planning Reports (e.g., resource utilization reports, etc.)
- Recommendations for improving operational efficiencies

3.5 CLIN 00003 – Applications

3.5.1 CLIN Type

This CLIN is firm-fixed price.

3.5.2 Place of Performance

For specific operations and maintenance actions requiring hands-on work or face-to-face, direct stakeholder interaction, the place of performance for this CLIN is at NETL sites Albany, OR, Morgantown, WV, and Pittsburgh, PA.

3.5.3 Objectives

The objective of the Applications CLIN is to conduct O&M using Systems Development Life Cycle (SDLC) processes by applying guidance from the Data Management Body of Knowledge (DMBOK) and Capability Maturity Model for Development (CMMI-DEV) and Data Management Maturity (DMM) maturity level 3 principles associated with patching, upgrades, defect correction, configuration changes, and requested development efforts for existing NETL Enterprise platforms, applications, and databases.

3.5.4 Scope

Applications activities, supporting existing NETL platforms, applications, research systems, and databases, includes:

- Platform and database maintenance, which includes optimization/tuning, upgrades and patching
- Application maintenance, which includes patching, upgrades, defect correction, business owner change requests to individual features/functions, and delivering new capabilities for existing systems
- Application maintenance processes, which includes management of O&M projects, requirements and user story elicitation, secure design, development, testing, performance tuning, cybersecurity hygiene, quality assurance, and system administration
- Creation of and updates to associated processes and SOPs (related to bullets 1 & 2 above), adhere to CMMI-DEV and DMM maturity level 3.

3.5.5 Requirements

- *The Contractor shall adhere to CMMI-DEV maturity level 3 processes* implementing integrated project management practices via PMI Agile or other disciplined agile methodologies and techniques for compliance; provided those SOPs and artifacts/deliverables are developed and maintained to support proper system development, integration, communication, and maintenance activities.

- *The Contractor shall maintain and administer existing NETL enterprise application, platform, and database management system capabilities* in accordance with CMMI maturity level 3 practices and apply industry best practices regarding administration capabilities, configurations, role-based access management, security, and scheduling of the latest market upgrades to ensure environmental integrity.

- *The Contractor shall provide solution development and administrative maintenance services for NETL's existing application portfolio* in accordance with CMMI-DEV maturity level 3 practices by adhering to Federal, DOE, NETL, and industry standards and best practices. The Contractor shall utilize NETL's current inventory of development tools and platforms when modifying existing interfaces, applications, and systems. Deviation from the current inventory of development tools, technologies, and platform, or any additions to the current software inventory, must be authorized by

NETL ITAB. Modified solution components must allow for reuse and minimize dependency on desktop/workstation configuration and the hosting environment. The Contractor shall ensure As-Built documents are maintained and brought current within 5 business days following release to production.

- *The Contractor shall provide business intelligence, operational reporting, data analytics, and ad hoc reporting support* to assist NETL business units and application end-users on an as-needed basis; providing analytics and reports not found natively within the environment by retrieving data from internal and external systems. The Contractor shall support creation, verification, release, and maintenance of data definitions for multiple business intelligence tools.

- *The Contractor shall contribute input and recommendations to improve and enhance NETL's existing Business Systems Roadmaps, Application/Technology Portfolios, process improvements, and automation of service capabilities.*

- *The Contractor shall elicit requirements/user stories associated with O&M* in accordance with CMMI-DEV maturity level 3 and PMI Agile methodology practices. This includes eliciting business requirements/user stories from stakeholders; analyzing to derive data, system, and software needs; documenting and maintaining necessary attributes for required levels of requirements; demonstrating business needs and desires are met through traceability matrices; and recommending allocation to the appropriate NETL business architecture components.

- *The Contractor shall contribute to and maintain a Requirements/User Story Repository* (tracking mechanism) in accordance with CMMI level 3 practices from which to manage business process, requirements and user stories developed by or provided to the IT organization for NETL's existing application portfolio. This repository must classify requirements and be available as a resource for referencing across all IT initiatives for assessing change and communicating the portfolio's existing business capabilities.

- *The Contractor shall provide thorough and effective data design and management services associated with O&M,* in accordance with the DMBOK and CMMI DMM maturity level 3 practices, which include data management planning, governance expertise, data modeling, database design, and data integration. The Contractor shall maintain database design artifacts to include logical and physical designs, data mappings, Interface Control Documents (ICDs) for each data interface, data dictionaries, and data management plans.

- *The Contractor shall contribute to and maintain a Test Case Repository* (tracking mechanism) from which to test all new and changed applications/systems thoroughly prior to deploying into production. The Contractor shall create test cases including user acceptance, regression, integration, unit, system, and data verification scenarios as required.

- *The Contractor shall support the NETL user community to enable maximum user participation during User Acceptance Testing (UAT)* related to O&M by performing the following activities related to UAT: Elicit business use scenarios from business stakeholders which upon a successful test outcome would generate acceptance from the business that requirements were met. Document user scenarios and provide in a format to be executed by the business; establish and maintain the UAT environment, including required datasets; participate with users during UAT by annotating test results and feedback; and compile UAT testing results and potential workarounds for review during deployment readiness meetings.

- *The Contractor shall conduct Release Management for the Test and Production environments* which ensures: change is managed by a formal change control process; validation testing (Integration, Regression, Security and UAT) is successfully conducted prior to release to the NETL production environment; a systematic approach to managing code, project artifacts, documentation, etc. relating to the software engineering environment at NETL for all system engineering efforts is maintained, including those developed by third-party development teams; IT technical architecture standards are communicated to solution providers; and release standards are establish, maintained and communicated to all solution providers deploying to the NETL environment.

- *The Contractor shall provide quality system, assurance, and control services* in accordance with CMMI-DEV maturity level 3 practices and ISO 9000/9001 by planning, executing, and managing verification and validation testing.

- *The Contractor shall collaborate with internal and external entities to ensure compliance with identified cybersecurity controls to protect information, prevent and mitigate threats, mitigate vulnerabilities, identify, and mitigate risks, and apply countermeasures.* Security requirements shall be considered throughout the O&M phase, thereby mitigating risk to minimize cost.

- *The Contractor shall provide support and input into the Enterprise Annual DRP* ensuring alignment with Federal policies, program standards, and guidelines.

- *The Contractor shall provide Tier 2 & 3 incident and request support for Enterprise applications* maintained by the IT site support contractor and for third-party developer/vendor support as required.

3.5.6 Performance Expectations/Inspection and Acceptance

The performance expectations for the Applications CLIN are summarized into performance objectives listed below followed by the performance expectation and the surveillance method. The performance expectation is the standard for which services will be accepted.

Performance Objective	Performance Expectation	Surveillance Method
The Contractor shall demonstrate mature SDLC practices.	The Contractor will demonstrate 95% compliance to the SDLC practices defined in alignment with CMMI DEV and DMM level 3.	NETL shall implement Quality Assurance Audits, minimally on a bi-yearly basis.
The Contractor shall ensure platform, application, and database services are operational.	The Contractor will ensure 99.5% uptime for the identified business systems, platforms, and underlying database services.	NETL shall receive monthly service uptime reports.
The Contractor shall perform all preventive maintenance activities within the IT environment without negatively impacting the NETL user community in accordance with the Annual Operations & Maintenance Plan.	The Contractor shall submit an Annual O&M Plan to the government for review and approval 60 days before the start of a new calendar year - 100% compliance.	NETL shall assess the degree to which the plans are submitted on-time through COR twice yearly audits, observation and review of the O&M schedule and plans.
The Contractor shall update each platform quarterly, at a minimum.	The Contractor will upgrade all identified platforms quarterly as indicated within the O&M Plan.	NETL shall verify through COR twice yearly audits, observation and review of the O&M schedule and plans.

3.5.7 Deliverables/Schedule

Quarterly O&M Plan – An Operations & Maintenance Plan delivered quarterly will indicate anticipated and planned efforts outlining the upcoming three months of initiatives including known upgrades, patches, technical debt reduction, platform upgrades, and prioritized requested business change needs.

Monthly Activity Report (MAR) – The Contractor shall provide a monthly report, preferably generated or automated, of the enterprise application activities including but not limited to:

- Initiatives Summary – current enterprise application initiatives, status, SDLC practice adherence, etc.
- Applications and Services Status Monitoring Summary – uptime, outages, service interruption reports, problems, corrective actions, etc., for all enterprise application services
- Tier 2/3 Service Desk Summary – tickets resolved by system, average ticket duration, etc.
- Production Change Release Summary – changes to the production environment performed by enterprise applications O&M resources
- Issues/Authorization – identified problems or outstanding artifacts requiring a response or assistance from the Government

4 CLIN 00004 – Cybersecurity

4.1 CLIN Type

This CLIN is firm-fixed price.

4.2 Place of Performance

For specific systems development processes/events requiring face-to-face, direct stakeholder interaction, the place of performance for this CLIN is at NETL sites Albany, OR, Morgantown, WV, and Pittsburgh, PA.

4.3 Objectives

The objective of the Cybersecurity CLIN is to protect the systems and data which NETL relies on from internal and external threats; support risk-based decision making which enables the lab to take advantage of new information management approaches and technology; and execute a cybersecurity strategy and implementation plan which supports mission priorities.

4.4 Scope

The Cybersecurity boundary of authority governs all systems covered by Enterprise including Research and Science Computing Services, as well as systems and applications which reside on NETL owned or operated infrastructure, including connections and interfaces to cloud services.

Cybersecurity scope encompasses all functions and services needed to ensure the Confidentiality, Integrity, and Availability of NETL's data and associated systems, prioritizing the following:

- Ensure NETL IT solutions are secure and available to support business operations in compliance with Federal, Departmental, and NETL policies and procedures.
- Develop and maintain cybersecurity program documentation and policies.
- Contribute to the design and maintain secure IT solutions based on those policies; and to protect, detect, respond, and recover the IT environment from cyber threats, compromises, weaknesses, and incidents.

4.4.1 Cybersecurity Program Support Services

The Contractor shall provide cybersecurity program support services. The Contractor shall provide the expertise, technical knowledge, staff support, and other related resources necessary to assist with meeting requirements defined below. The Contractor staff shall have knowledge, skills and abilities to support NETL provided Cybersecurity tools and technologies.

The Contractor shall ensure that all areas of IT work meet mandated cybersecurity requirements.

The Contractor shall provide services to develop, operate, and maintain an effective and regulatory-compliant cybersecurity program for NETL. The program requirements include maintaining existing FISMA system certifications and accreditations, continuous monitoring of the FISMA systems; mandatory reporting (e.g., FISMA, OCIO, Office of Management and Budget); network intrusion detection, prevention and monitoring; incident response handling and reporting; continuity of operations planning and testing; cybersecurity policies and guidance; continuous cybersecurity awareness training; protection of PII; and compliance with OCIO, National Institute of Standards and Technology, and applicable government regulations and guidelines. The Contractor shall maintain open communication on all cybersecurity–related incidents and activities with federal IT/Cyber staff.

The Contractor shall establish a structure to capture costs consistent with capital planning budget guidance tracked at Identify, Protect, Detect, Respond and Recover detail level for IT Security and Compliance.

The objective is to provide cybersecurity planning, reporting, and implementation to ensure the adherence to Federal and Departmental cybersecurity requirements. Specific requirements include but are not limited to:

- The Contractor shall provide guidance and expertise on Federal policies, program standards, and guidelines such as, but not limited to, those listed below, or later versions as amended:

REFERENCE	DESCRIPTION / TITLE
FISMA	*Federal Information System Modernization Act (FISMA) (2014)*
FIPS 199	*Federal Information Processing Standards (FIPS) Publication 199 - Standards for Security Categorization of Federal Information and Information Systems*
FIPS 200	*Minimum Security Requirements for Federal Information and Information Systems*
NIST SP 800-30 Rev 1	*National Institute of Standards and Technology (NIST) Guide for Conducting Risk Assessments*
NIST SP 800-35	*Guide to Information Technology Security Services*
NIST SP 800-37 Rev 2	*Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*
NIST SP 800-39	*Managing Information Security Risk: Organization, Mission, and Information System View*
NIST SP 800-44 Version 2	*Guidelines on Securing Public Web Servers*
NIST SP 800-53 Rev 4	*Security and Privacy Controls for Federal Information Systems and Organizations*
NIST SP 800-53A Rev 4	*Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans*
NIST SP 800-61 Rev 2	*Computer Security Incident Handling Guide*
NIST SP 800-83 Rev 1	*Guide to Malware Incident Prevention and Handling for Desktops and Laptops*
NIST SP 800-86	*Guide to Integrating Forensic Techniques into Incident Response*
NIST SP 800-101 Rev 1	*Guidelines on Mobile Device Forensics*
NIST SP 800-115	*Technical Guide to Information Security Testing and Assessment*

REFERENCE	**DESCRIPTION / TITLE**
NIST SP 800-128	*Guide for Security-Focused Configuration Management of Information Systems*
NIST SP 800-137	*Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*
NIST SP 800-150	*Guide to Cyber Threat Information Sharing*
NIST SP 800-153	*Guidelines for Securing Wireless Local Area Networks (WLANs)*
NIST SP 800-160 Vol 1	*Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*
NIST SP 800-171 Rev 1	*Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*
NIST SP 800-171A	*Assessing Security Requirements for Controlled Unclassified Information*
NIST SP 800-181	*National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework*
P.L. 93-579	*Public Law 93-579 Privacy Act, December 1974 (Privacy Act)*
40 U.S.C. 11331	*Responsibilities for Federal Information Systems Standards*
OMB M-19-03	*Office of Management and Budget (OMB) Memorandum 19-03, Strengthening the Cybersecurity of Federal Agencies by enhancing the High Value Asset Program*
OMB A-130	*OMB Circular A-130, Managing Information as a Strategic Resource*
BOD 18-02	*Department of Homeland Security's Binding Operational Directive 18-02, Securing High Value Assets*
BOD 19-02	*Department of Homeland Security's Binding Operational Directive 19-02, Vulnerability Remediation Requirements for Internet-Accessible Systems*
DOE Order 205.1C	*Department of Energy Cybersecurity Program*

- The Contractor shall provide advisory support to the Government for managing the risk posture of the environment and continuous monitoring activities including understanding weaknesses, their potential impact, and corrective action plans and make risk mitigation recommendations to the Authorizing Official (AO)/Authorizing Official Designated Representative (AODR).
- The Contractor shall support the mandated implementation of the DHS Continuous Diagnostics & Mitigation (CDM) program at NETL.
- The Contractor shall annually support, plan to remediate, and address identified findings in all NETL environments by independent assessments.
- The Contractor shall support third party FISMA Compliance and Security Architecture Audits, penetration tests, and Site Assistance Visits (SAVs).
- The Contractor shall provide expertise to secure and monitor applications and infrastructure running in on-premises and cloud environments in accordance with Government defined standards and within Government defined frameworks.
- The Contractor shall provide support and input into the Enterprise and Research Annual DRPs ensuring alignment with Federal policies, program standards, and guidelines.

4.4.2 Risk and Vulnerability Assessments

The Contractor shall provide Risk and Vulnerability Assessment (RVA) services. The Contractor shall conduct assessments of threats and vulnerabilities, determines deviations from acceptable configurations, enterprise, or local policy, assesses the level of risk, and develop and/or recommend appropriate mitigation countermeasures in operational and non-operational situations. RVA services include, but are not limited to: Network Mapping, Vulnerability Scanning, Phishing Assessment, Wireless Assessment, Web Application Assessment, Operating System Security Assessment (OSSA), and Database Assessment.

- The Contractor shall perform network mapping to identify assets on agreed-upon IP address space and network ranges.
- The Contractor shall perform vulnerability scanning which comprehensively identifies IT vulnerabilities associated with NETL systems that are potentially exploitable by attackers.
- The Contractor shall perform regularly recurring phishing assessment activities to evaluate the level of awareness of the NETL workforce regarding digital forms of social engineering. This activity includes assessment with scanning, testing, phishing email events, and awareness campaigns over several months.
- The Contractor shall perform wireless assessments including WAP detection, penetration testing, and other methods as needed while onsite at NETL facilities.
- The Contractor shall perform web application assessments involving scanning and testing of both outward facing and internal web application for defects in web site or web service implementations which provide mechanisms for exploitable vulnerabilities. Reports will be provided on how web services can be provided securely and what techniques can be used to limit access and responses to legitimate requests.
- The Contractor shall perform Operating System Security Assessments (OSSA) for the configuration of select host operating systems against standardized configuration baselines.
- The Contractor shall perform database assessments for the configuration of selected databases against configuration baselines to identify misconfigurations or database vulnerabilities.

4.4.3 Cyber Hunt

The Contractor shall provide and perform Cyber Hunt capabilities. Cyber Hunt activities include continuous and ongoing activities to monitor Indicators of Compromise, assess threat intelligence, and assist with responses to crisis or urgent situations within the pertinent domain to mitigate immediate and potential threats.

- The Contractor shall use information and threat intelligence specifically focused on the proximate incident to identify undiscovered attacks and/or indicators of compromise, and shall investigate and analyze all relevant response activities.
- The Contactor shall collect intrusion artifacts (e.g., source code, malware, and trojans) and use discovered data to enable mitigation of potential Computer Network Defense incidents within the enterprise.
- The Contractor shall coordinate with and provide expert technical support to enterprise-wide network defense technicians to resolve network defense incidents.
- The Contractor shall correlate incident data to identify specific vulnerabilities and provide recommendations to Incident Response that enable expeditious remediation.

4.4.4 Incident Response

The Contractor shall provide Incident Response services. Incident Response services respond to a compromise, determine the extent of the incident, remove the adversary from their systems, and restore their networks to a more secure state.

- The Contractor shall perform command and control functions in response to incidents utilizing the intrusion artifacts collected during Cyber Hunt.
- The Contractor shall engage necessary technical resources to expeditiously remediate and execute recommendations resulting from correlated incident information and monitor resulting activities through resolution.

4.4.5 Penetration Testing

The Contractor shall provide Penetration Testing services. Penetration Testing is security testing in which assessors mimic real-world attacks to identify methods for circumventing the security features of an application, system, or network.

- The Contractor shall conduct and support authorized penetration testing on enterprise network assets.
- The Contractor shall analyze NETL network defense policies and configurations in addition to evaluating compliance with regulations and enterprise directives.
- The Contractor shall assist with the selection of cost-effective security controls to mitigate risk (e.g., protection of information, systems, and processes).

4.4.6 Information Assurance

The Contractor shall provide information system authorization and information assurance support. Contributions to system authorization and information assurance support include, but are not limited to: leading the creation of A&A packages, system security plans, Plan of Actions and Milestones (POAMs), privacy assessments, data categorizations, and ATO artifacts. The Contractor shall collaborate directly with Enterprise and Research Information Systems Security resources to deliver quality artifacts aligned with the Risk Management Framework and industry best practices mapping documented security requirements to both planned and realized security controls. The Contractor shall deliver an information assurance wellness plan identifying missing artifacts and gaps in content within existing artifacts targeting the remediation and improvement of the lab's adherence to binding directives, regulations, and the Risk Management Framework. The Government shall review the wellness plan, provide feedback, and prioritize initiatives for artifact remediation. The Contractor shall remediate system authorizations and information assurance artifacts in alignment with the agreed upon IA wellness plan.

4.5 Performance Expectations/Inspection and Acceptance

The performance expectations for the Cybersecurity CLIN are summarized into performance objectives listed below followed by the performance expectation and the surveillance method. The performance expectation is the standard for which services will be accepted.

Performance Objective	Performance Expectation	Surveillance Method
Vulnerability Management	The Contractor shall conduct ongoing (continuously monitor) and periodic (no less than monthly) vulnerability scans against internal, cloud (IaaS, PaaS, SaaS), and public-facing systems.	NETL shall receive monthly vulnerability mitigation reports.
Quarterly Incident Response Exercise	The Contractor will work with NETL IT and ITSS staff to conduct quarterly table-top exercises (TTX) to address POAMs in alignment with the Incident Response Plan.	NETL shall implement an Incident Response Exercise on a quarterly basis.
Monthly Cybersecurity Status Report	Includes statistics on incidents, continuous monitoring efforts, initiatives, graphs, charts, and trend analysis, including Indicators of Compromise, correlated events, vulnerabilities and mitigations, and incident response metrics.	NETL shall receive monthly Cybersecurity status reports.

Software/solution scanning	Conduct targeted solution scanning, within 3 business days of request, to ensure effective and timely support to IT solution providers.	NETL shall monitor request/response tickets for timely scanning support.
Data Calls	Respond to Quarterly (and ad hoc) FISMA/OMB/HQ reports – Content dependent upon report.	NETL shall implement Quality Assurance Audits, quarterly with 100% inspection of scheduled and ad hoc data calls.
Enterprise Business Impact Assessment (BIA)	The Contractor shall assist NETL IT to conduct an enterprise-wide Business Impact Analysis (BIA) identifying High Value Assets (HVAs) and criticality of NETL systems.	NETL shall implement a Quality Assurance Audit on a bi-yearly basis.
Information System Authorizations	The following System Authorization documentation is maintained and regularly revised in compliance with departmental requirements: • Risk Assessment • System Security Plan • Security Assessment Report • Plan of Actions and Milestones • Privacy Needs Assessment • Privacy Impact Assessment • Configuration Management Plan • Contingency Plan • Continuous Monitoring Plan • Authorization Letter	NETL shall implement a Quality Assurance Audit on a bi-yearly basis (includes all historical authorizations plus any new authorizations over prior six months).

4.6 Deliverables/Schedule

- **IA Wellness Plan -** An Information Assurance Wellness plan will indicate a plan for refreshing all NETL ATOs, information system authorizations (i.e., A&A packages), and identifying missing required information assurance documentation for effort prioritization. A wellness plan is expected to be delivered initially 90 days following contract award. Twice per year, the wellness plan will be updated with progress on the overall health and improvements in NETL's information assurance documentation incorporating any new audit findings, additional information systems identified, etc.
- **Annual NETL Risk Management Framework Update**
- **Annual Incident Response Plan (IRP) -** The Contractor shall provide a recommended annual incident response plan providing guidelines for rapid response and resolution using a unified, standardized approach for handling security incidents, incident detection, reporting, analysis, prioritization, and resolution.
- **Baseline Documentation (as required)**

- **Assessment & Authorization packages (as required)**
- **Plans of Actions and Milestones (as required)**
- **Monthly Cybersecurity Status Report** – Includes statistics on incidents, continuous monitoring efforts, initiatives, etc.
- **Quarterly (and ad hoc) FISMA/OMB/HQ reports** – Content dependent upon report.

5 CLIN 00005 – Research

5.1 Background

The Research IT environment provides the capabilities, services, systems, tools, and infrastructure to support high performance computing and artificial intelligence and machine learning research of the laboratory. Research IT collectively represents a critical capability underpinning NETL's R&D portfolio and is defined as hardware, information systems, software, and the personnel required to maintain these resources to support NETL's mission for applied energy research and scientific discovery. Research IT provides two specialized high performance computing platforms: Joule 2.0 (NETL's supercomputer) and modular data center in Morgantown, and a purpose-built cloud system designed for data analytics and machine learning (ML) called Watt, which is the main platform supporting Center for Artificial Intelligence and Machine Learning (CAML) in Pittsburgh. Research IT also encompasses virtual data creation and collaboration services called EDX in Morgantown and in public cloud service providers, as well as high-speed, low-latency networking; special-purpose computing for data collection and analysis; domain-specific software. More details are described in the following sections of Activity 00005a - High-Performance Computing (HPC) and Activity 00005b - Energy Data eXchange (EDX).

5.2 Scope

The Contractor shall provide capabilities including experience, skills, and personnel to maintain, operate and integrate solutions for Research Computing, which includes High-Performance Computing (HPC) and Energy Data eXchange (EDX).

The Contractor shall be responsible for research information systems security functions for the Research environment. The requirements shall include, but are not limited to:

- Analyze design constraints, trade-offs, and detailed system security.
- Serve as a principal advisor on all matters, technical and otherwise, involving security controls for each system.
- Assist in the development of the system-level security, which may include, but is not limited to, physical and environmental protection; personnel security; incident handling; and security and privacy training and awareness of both system owners and IT support staff.
- Lead, organize support, execute, and directly contribute to Risk Management Framework assessment and authorization (A&A) packages for Research systems, subsystems, and environments, when necessary and in collaboration with the respective system owners.
- Document any modification or deviation from organizationally defined security policies and standards (e.g., FISMA, NIST, etc.) as well as the resulting risks and any recommended mitigation actions for Authorizing Official or Designated Representative approval.
- Protect information and information systems from unauthorized system activity or behavior to provide confidentiality, integrity and availability of information and systems.
- Contribute to Disaster Recovery and Continuity of Operations Plans for systems under development and ensure testing prior to new systems entering a production environment.
- Interface with Government Cybersecurity staff and third-party assessors as needed on data calls, audits, and assessments.
- Interface with Government Architects and Contractor architect support personnel to ensure security control integration into overall system designs.

5.3 Activity 00005a – High Performance Computing (HPC)

5.3.1 Activity Type

This Activity is cost-plus award fee.

5.3.2 Place of Performance

For operations and maintenance actions requiring hands-on work or face-to-face, in-person stakeholder interaction, the place of performance for this CLIN is at NETL sites Morgantown, WV, Pittsburgh, PA, and Albany, OR.

5.3.3 Objectives

The objective of the Activity is to provide contractor support for the NETL High-Performance Computing (HPC) Infrastructure, including Joule Supercomputer and Watt Cloud, and the support of Artificial Intelligence (AI)/Machine Learning (ML), at the National Energy Technology Laboratory (NETL).

The NETL Supercomputing infrastructure, Joule, is configured specifically to meet the needs of materials science, chemistry, geoscience, and fluid dynamics research. NETL's supercomputing capability enables researchers to simulate phenomena that are difficult or even impossible to otherwise measure and observe and reduces the cost and time of technology development at every stage by speeding up the discovery of new materials, increasing the reliability and performance of novel devices, and reducing the risk inherent in scaling-up processes. Joule 2.0 is in the Modular Data Center (MDC), and the new Joule 3 is planned for installation in the MDC, Morgantown, in the Fall 2023 with an option to move to new Computational Science & Engineering (CSE) Center, Morgantown, once the CSE building is ready in 2026.

The NETL Cloud infrastructure, Watt, is NETL's private IaaS/PaaS cloud computing environment. Watt is intended to allow NETL to explore problems in ML, AI, data mining, and data analytics. It was specifically designed to support machine learning and data analysis workflows by allowing researchers to create virtual machines and house, move, and process multiple petabytes of data using a variety of algorithms developed in-house and with corporate and university research partners. This facility enhances NETL's ability to combine physics-based modeling and AI and ML to efficiently provide solutions to problems that are too intricate for standard computing. Watt is hosted in B-94, Pittsburgh, and Watt is anticipated to be expanded and refreshed at a new Center for Artificial Intelligence and Machine Learning (CAML), B-83, Pittsburgh, in late 2024.

5.3.4 Scope and Requirements

HPC encompasses all the functions and services that are needed for support of the NETL HPC, including infrastructure, network, data, and application services. The Contractor shall provide personnel with technical expertise in HPC Services which are built and managed upon a framework that includes lifecycle planning, designing, obtaining, documenting, installing, securing, operating, maintaining, improving, changing, controlling, and decommissioning of HPC assets.

The Contractor shall be responsible for supporting HPC specific requirements, in addition to the Governance and Overarching Support laid out in Section 2 - General Contract Requirements. The HPC requirements consists of six support areas: (1) HPC Solutions Architect Support, (2) HPC Service Operations Support, (3) HPC Service Improvement & Modernization Support, (4) HPC Data Center Facility Operations & Maintenance Support, (5) HPC Service Desk Support, and (6) HPC Service Purchasing Support.

Essential HPC services – HPC Service Operations Support and HPC Data Center Facility Operations & Maintenance Support – are required to be available and operational 24 hours a day, 7 days a week, 365 days a year, even during site closings for weather. During NETL business operation hours, it is expected that the loss of Essential HPC services shall result in immediate (within 15 minutes) response times for remediation. If necessary to restore service per Government direction, have staff on-site within three hours of initial contact to troubleshoot and resolve the service interruption or identified problem.

5.3.4.1 HPC Solutions Architecture Support

The Contractor shall provide HPC Solutions Architect Support. HPC is anticipated to be refreshed or upgraded every three to five years. The objective is to provide strategic planning and design support in such a manner as to improve and develop modern HPC over the long term as directed by NETL, through appropriate design choices, proper upgrades, and timely refreshes. The Contractor shall develop plans that define how the Contractor's HPC solution will operate and adapt to changes throughout the course of performance. Specific requirements include but are not limited to:

- The Contractor shall provide engineering and technical expertise to aid the development of technical requirements packages in the design, development, implementation, operations, and maintenance for the hardware/software refresh of the HPC, including full or partial refresh of HPC, Joule and Watt. The Contractor shall support authorized HPC-related purchases such as equipment, software, maintenance agreements, licenses, etc.
- The Contractor shall assess emerging technologies and disruptive technologies to determine their suitability for the HPC operating environment.
- The Contractor shall support the development of proofs-of-concept and pilot programs to explore the viability and potential effectiveness of new technologies for use within the HPC environment.
- The Contractor shall analyze the current HPC architecture and business needs, identify deficiencies, issue recommendations on new and emerging HPC trends, and draft information, technology, security, and artifacts.
- The Contractor shall document industry trends, including third-party assessment tools, conduct and document analyses of alternatives before presenting a recommended solution. The Contractor shall specifically be responsible for preparing and maintaining any operational/architecture drawings/diagrams which facilitate the documentation and understanding of the HPC systems and supporting processes.
- The Contractor shall provide a communication plan to ensure the lines of communication between the Contractor and the Government remain open and available, to include regular and ad hoc reports, meetings, and briefings with stakeholders. The Contractor shall perform requirements intake for stakeholders, acting as the primary interface for the initiation and management of in-house HPC Projects.

5.3.4.2 HPC Service Operations Support

The Contractor shall support HPC Service Operations. The objective is to keep the NETL HPC infrastructure, system, and services fully functional and optimized to deliver quality services to the HPC users. The HPC Service Operations Support includes, but is not limited to, the following specific requirements: (a) Compute and Storage Operations, (b) Network Operations, (c) Virtualization, OS, Middleware, Runtime, and Application, (d) Data Management & Analytics, (e) Account Management, and (f) Cybersecurity Operations Support as follows:

HPC Compute and Storage Operations Support

- The Contractor shall provide solutions to provide and/or support solutions capable of supporting physical and virtual HPC servers for NETL's application and data storage needs. The Contractor shall ensure the solution can scale compute capabilities appropriately in terms of central processing unit (CPU) processing power, graphics processing unit (GPU), available memory, and available storage space, to accommodate surges in usage or data.
- The Contractor shall maintain both CPU-only and CPU/GPU Compute Nodes and Storage Nodes. Joule 2.0 is consisted of 40 racks of approximately 2,000 compute and storage nodes. Watt is consisted of 19 racks (13 server racks and 6 vertical cooling racks) with 39 storage nodes (40PBs

of raw storage), 24 CPU/GPU compute nodes, and 8 CPU-only pool servers.

- The Contractor shall support new AI infrastructure as well such as, but not limited to, wafer-scale engine (WSE) to support AI, ML and Deep Learning (DL) for NETL AI/ML research.
- The Contractor shall maintain Storage such as, but not limited to, Serial Attached SCSI (SAS) Hard Disk Drive (HDD) storage and Non-Volatile Memory Express (NVMe) Flash storage.
- The Contractor shall maintain Short-term and Long-term file system using Lustre parallel distributed file system, and Network File System (NFS) as well as Robinhood (or equivalent) Policy engine. Various file system and file transfer protocol should be managed. Long-term file system should be housed in a separate, physically segregated, data center with backup power generation to make storage of data as safe as possible. Current Joule 2.0 long-term backup storages are located in B-39 data center, Morgantown.
- The Contractor shall provide operations and maintenance support for installation and deployment such as racks, cables, etc., tuning and optimization for computational hardware such as HPC compute nodes, storage/backup nodes, and user interface and maintenance nodes.
- The Contractor shall provide Legacy Support. The Contractor shall assume responsibility of the current, Government-owned systems and end user environment, which shall include HPC infrastructure and services. Requirements for supporting the current environment shall include management and maintenance of the existing infrastructure and ensure legacy HPC systems interoperate and work seamlessly with Contractor-provided services.

- The Contractor shall address incident, Problem and Event Management described in Section 2 - General Contract Requirements. The Contractor shall resolve HPC problems, such as, but not limited to, diagnosis and repair of faulty HPC hardware components, and request for the replacement components to vendors such as Power Distribution Board (PDB), Backplanes, Dual In-line Memory Module (DIMM)/Random Access Memory (RAM), AUX/EFUSE, HDD, etc. Ensure that all HPC production is always within the original manufacturer's equipment warranty or under vendor support maintenance agreements.

HPC Network Operations Support

- The Contractor shall provide managed network services such as addition and maintenance of infrastructure, network configuration services, network monitoring and management, and incident management and response.
- The Contractor shall support Computational Network, Access Network, and Maintenance Network management including Cable Management, Network Switching/Routing/Virtualization, and VLANs to ensure efficient network flow of data.
- The Contractor shall manage Computational Network Interconnects within HPC cluster using diverse network technologies such as, but not limited to, 100Gbps, 200Gbps, 400Gbps, or faster, low-latency network using diverse vendor products.
- The Contractor shall manage connections through Science LAN, Research LAN, Admin LAN, and Foreign National LAN over all three sites, Morgantown, Pittsburgh, and Albany.
- The Contractor shall manage connections among HPC systems, Joule, Watt and Energy Data eXchange (EDX), *[Activity 00005b]*. EDX and Science LAN data should be periodically backed up onto CAML/Watt Storage. Watt Storage has been split into two; One (37 storage servers) is dedicated to Watt home directory and volumes/shares in CAML and the other one (2 storage servers) is dedicated to EDX/Science LAN backup storage which is temporarily located in PGH-B922 data center with CPU-only pool servers until backup Generator is ready for CAML.
- The Contractor shall provide External Network Management. The Contractor shall manage connections to HPC, from Off-Site Public Internet through TIC and DOE's Energy Sciences Network (ESNET), a high-speed computer network serving DOE scientists and their collaborators worldwide to support NETL scientific research and to ensure efficient network flow of data.
- The Contractor shall provide VPN services and ensure that VPN access requires multi-factor authentication and is appropriately secure, and that it provides access to all operating systems supported in the environment.
- The Contractor shall provide Ethernet Infrastructure Controllable via Intelligent Platform

Management Interface (IPMI) or equivalent; connections to nodes must be 1Gbps or faster; Ethernet network must be a tree configuration using 10G or faster core switches. All switches must be compatible and supported on existing infrastructure.

- The Contractor shall provide Network Services such as DNS, DHCP, NTP, Hypertext Transfer Protocol Secure (HTTP/HTTPS), SMTP, NNTP for HPC.
- The Contractor shall provide HPC Network Security & Control such as Firewall Services, Network Access Control (NAC), Network Segmentation, Intrusion Detection System (IDS) / Intrusion Prevention Systems (IPS).
- The Contractor shall provide IP Address Management for HPC including IPv6 Transition Implementation to migrate all NETL assets to use Ipv4/Ipv6 dual stack or Ipv6 only with NAT64 to communicate with Ipv4 only.
- The Contractor shall perform the requirements to follow Enterprise Infrastructure Network guidance *[CLIN 00002]*. The Contractor shall maintain network infrastructure, in accordance with current technology standards and all applicable Federal and Department regulations. The Contractor shall ensure that all managed internet services are provided through a Trusted Internet Connection Access Point (TICAP) or ESNET and are in compliance with all applicable requirements. The Contractor shall collaborate with Enterprise Infrastructure team for fiber jumpers' cutover/move/installation, to provide seamless HPC network and service delivery.

HPC Virtualization, OS, Middleware, Runtime, and Application Support

- The Contractor shall provide HPC management, including underlying Operating System (OS; Unix/Linux and Windows), Virtualization/Hypervisor & Containerization, Middleware, Runtime, and Application Layers. Management expectations include installation, deployments, packaging, configuration, compilation, debugging, upgrades/renewal, and refresh.
- The Contractor shall support in-house, Open-Source, or commercial off-the-shelf (COTS) HPC Software Maintenance such as, but not limited to:
    - HPC/Joule Cluster Management Tool with Queues and Scheduling (QoS and Limits), Partitions, and Group management.
    - HPC/Watt Open-Source Cloud Computing Infrastructure and Management Tool and Virtualization/Containerization technologies including multi-node cluster setup with virtual machine, container, or bare-metal CPU/GPU compute nodes.
    - HPC Simulation-Based Engineering Tools/Applications and Parallel Programming language and numeric computing environment for materials science, chemistry, geoscience, and fluid dynamics research.
    - ML and AI software framework and libraries, used to train and deploy deep neural networks, including programming languages for scientific computing and data-science packages.
    - The Contractor shall build executable code from source code.
    - The Contractor shall analyze solution alternatives and recommend the best implementation to meet HPC customer requirements.
    - The Contractor shall manage connection and configuration for the software license server located both in-HPC and outside of HPC Datacenter. Some software licenses are installed in the Science LAN or Shared Enterprise Network_Science LAN (SEN_SCI) Network where a centralized license server is located for Research software.
    - The Contractor shall provide automated software detection and license monitoring services for all software. The Contractor shall be responsible for tracking HPC software license/agreements and notifying the TCOR of the expiration within 90 days.
- The Contractor shall provide Development-Operations (DevOps) and Performance Monitoring support.
    - The Contractor shall run High-Performance Benchmark with HPC vendor(s) to submit NETL HPC/Joule performance to the biannual TOP500 supercomputer list, whenever running the benchmark and achieving a better result.
    - The Contractor shall develop new software/scripts for HPC maintenance support.
    - The Contractor shall support HPC Access Client application including development,

maintenance, and upgrade for HPC connection through Internet and NETL LANs. HPC system should be secured through MFA and encrypted SSH tunnel connection through HPC Access Client.

  - The Contractor shall create and/or update HPC Client Documentation, including user manuals and training materials to accurately reflect the operation and use of software effectively in the HPC environment.
  - The Contractor shall ensure that vigilant monitoring standards apply to HPC systems, and actively engage in maintenance of hosted HPC environments. Ensure that all security and operational patches are applied as necessary while maintaining a controlled HPC environment.

HPC Data Management & Analytics Support

- The Contractor shall support Data Management & Analytics services by providing Data Science/Engineering services to HPC users within data analytics, data mining, and ML/DL to drive the Research mission. This service is to create a data pipeline, move the data, and then cleanse the data for making the data accessible and available to the researchers and developing algorithms for AI/ML.
- The Contractor shall provide expertise for the development of a data warehouse ecosystem for the support, management, and security of research data (experimental and simulation data) and high-performance data analytics with an emphasis on overall system performance.
- The Contractor shall develop to accommodate storage, analysis, and visualization of massive volumes of data expected to be accumulated within computational evaluation, optimization, and screening of large datasets of existent and artificially designed materials.
- The Contractor shall work directly with NETL researchers to determine data management needs and develop a business case in support of research data management.
- The Contractor shall evaluate and recommend computational models and algorithms to support NETL AI/ML research efforts.
- The Contractor shall perform data backup, archive, and restoration services. HPC data backup jobs will be organized, managed, and monitored. The Contractor shall ensure secure, robust, and reliable HPC data recovery services.

HPC Account Management Support

- The Contractor shall support Directory Service for HPC by managing Lightweight Directory Access Protocol (LDAP) and Samba on Linux to authenticate and authorize all HPC users and computing resources in domain type network, assigning and enforcing security policies.
- The Contractor shall provide Account Management with MFA, a security mechanism which requires an individual to provide two or more credentials to authenticate HPC users' identity.
- The Contractor shall program MFA RSA Token (cryptosystem for public-key encryption) and deliver to HPC users. The Contractor shall support the existing RSA Token for HPC.
- The Contractor shall ensure no unauthorized access to the HPC services. All evaluated privileged accounts shall have Government approval prior to creation and shall ensure that user accounts and permissions are granted and created using the HPC user account procedures.

HPC Cybersecurity Operations Support

- The Contractor shall support all work in accordance with cybersecurity mandates and directives according to the Section 2 – General Contract Requirements.
- The Contractor shall establish and maintain appropriate firewalls and security protocols to implement HPC security requirements. The Contractor shall support virus/malware/vulnerability prevention & remediation and data encryption.
- The Contractor shall be responsible for the implementation and verification of all cybersecurity controls for the HPC.
- The Contractor shall ensure all hosted servers are patched and maintained according to the most

current vendor release levels, and that all hosted servers comply with Federal and Departmental standards for cybersecurity.
- The Contractor shall support Security A&A for FISMA ATO (Low/Moderate) for HPC systems. The Contractor shall provide all documentation necessary to prepare a complete Risk Assessment, System Security Plan, Security Assessment Report, POA&M, PIA/PNA, CMP, Contingency Plan in support of ATO declarations for HPC systems.
- The Contractor shall ensure that all Personally Identifiable Information (PII) and other sensitive data are not stored on HPC.
- The Contractor may be required to ensure compliance with High Performance Computing Security Mandates established by NIST.

5.3.4.3 HPC Service Improvement & Modernization Support

The Contractor shall support Continual Service Improvement & Modernization for HPC, in addition to all Governance and Overarching Support laid out in the Section 2 – General Contract Requirements. The objective is to continuously improve capabilities, performance, and reliability of the HPC and to deploy changes/transition into the HPC environment successfully while minimizing the impact upon the quality and availability of the HPC to customers. Specific requirements include but are not limited to:

- The Contractor shall proactively recommend changes and/or enhancements to the HPC systems to provide better efficiency, productivity, stability, and/or cost savings within the larger scope of each project's scientific and engineering design requirements.
- The Contractor shall support utilization and capacity planning for HPC resources and monitoring tool to identify consumption trends and shall be responsible for providing recommendations for equipment and service replacement, upgrade, or enhancement to prevent the delivery of services from falling below acceptable performance levels.
- The Contractor shall perform all preventive maintenance activities within the HPC without negatively impacting the HPC user community. This preventative maintenance includes but is not limited to patching, updates, and version control.
- The Contractor shall expand and improve the HPC as necessary to provide service to HPC users and to adapt to changing mission capabilities and priorities. The Contractor shall support system transition on to and off the HPC as dictated by NETL.
- The Contractor shall support Infrastructure Modernization by replacing end-of-life equipment to support basic physical (hardware) and logical (software) layers.
- The Contractor shall support Technology Migration Planning to a to-be environment. The Contractor shall note that some elements of the as-is HPC environment are ongoing and will not be phased out, and the Contractor shall continue to support these elements, and propose a plan to migrate from the current HPC to a future-state HPC environment. The Contractor shall work with stakeholders to decommission the current HPC service(s) and migrate to the new HPC service, minimizing disruptions to end users and ensuring that customer satisfaction is measured and maintained.

5.3.4.4 HPC Data Center Facility Operations & Maintenance Support

The Contractor shall provide HPC Data Center Maintenance, Safety, and Security Support. Specific requirements include but are not limited to:

- The Contractor shall ensure that all HPC compute nodes, storage nodes, interface and maintenance nodes, and networks are fully monitored at all times using HPC monitoring tool and MDC environments (louvers, fans, actuators, PLC pars, remote I/O parts, etc.) are fully monitored by MDC monitoring tool, with automatic notifications configured to immediately alert staff of problems or failures. The Contractor shall maintain HPC/MDC monitoring tools used to monitor the health status and availability of all HPC environments. Upon detection of problems or failures, the Contractor shall perform immediate remedial actions to stabilize or restore the associated HPC services and notify Federal designee of the problems or failures.

- The Contractor shall support the monthly, quarterly, semi-annual, and yearly MDC maintenance operation/task. The Contractor shall support the semi-annual Joule Maintenance, in Spring and Fall, in conjunction with the semi-annual MDC maintenance.
  - MDC Control System Maintenance including Programmable Logic Controller (PLC), Human Machine Interface (HMI), and Supplemental Cooling for automation, notification, and enhanced self-protection features.
  - UPS Battery and System maintenance to protect from electrical surges/fluctuations, and Gasket, filter, evaporative media, and doors maintenance, and material purchasing.
  - Critical Spares Management: louvers, fans, actuators, PLC pars, remote I/O parts, etc.
  - Emergency Repairs: additional maintenance contract to provide NETL with the ability to call for repairs at any time to obtain immediate attention when required.
  - Joule Maintenance including workload manager upgrade for feature enhancements and fixes, remote server management tool maintenance, outstanding hardware and software maintenance, etc.
  - The Contractor shall collaborate with Morgantown Facility/Site Management and Environmental, Safety & Health (ES&H) & Emergency Management team for UPS/Generator/Cooling installation and maintenance for Joule/MDC.
- The Contractor shall support the semi-annual Watt/CAML Maintenance, Pittsburgh-B-94. The Contractor shall collaborate with Pittsburgh Facility/Site Operations/Management team for Semi-Annual UPS Maintenance, Fire Suppression System Inspection, Cooling/Power Maintenance, planned/unplanned outages, etc.
- The Contractor shall support New Co-Location Data Center Maintenance – CCSE (Center for Computational Science & Engineering), Morgantown and B-83 CAML, Pittsburgh. The CCSE is anticipated to be ready in 2026 and B-83 CAML is anticipated to be ready in late 2024. The Contractor shall collaborate with Enterprise Infrastructure Data Center team *[CLIN 00002]* for Rack Space Management & Cabling and Morgantown/ Pittsburgh Facility/Site Operations/Management team for Data Center Maintenance – Power, Cooling, UPS Management and Fire Suppression System Inspection.
- The Contractor shall support Data Center Move/Transition Support. The Contractor may be requested to support decommissioning, moving, and installation of HPC equipment to new Data Center, retrofit interface cards and cables, migrate HPC resources, and reconfigure the HPC environments.
  - Joule HPC Support for Data Center Transition from MDC to CCSE, Morgantown
  - Watt HPC Support for Data Center Transition from B-94 to B-83, CAML, Pittsburgh
- The Contractor shall support HPC Data Center Security & Safety Operations:
  - Physical Access Management: The Contractor shall ensure no unauthorized access to the HPC Data Center. All evaluated privileges shall have Government approval prior to access and shall ensure that permissions are granted and created.
  - Safety Management: The Contractor shall support safety management in accordance with NETL's safety mandates such as Safety Analysis and Review System (SARS) support operations including Activity Hazard Analysis (AHA).
- The Contractor shall support HPC Data Center Optimization and Cleaning.
- The Contractor shall maintain and report Data Center metering, energy efficiency, and risk assessments. The Contractor shall provide monthly and quarterly Power Usage Effectiveness (PUE) information including Total HPC Power (KW) and Total Data Center Power.
- The Contractor shall support Site Tours of the HPC Data Center to NETL visitors including federal agencies, state, local, and tribal government, and others as dictated by NETL.

5.3.4.5 HPC Service Desk Support

The Contractor shall provide HPC Service Desk Support. The objective is to supply rapid resolutions to HPC user incidents (which include events that cause or may cause an interruption or reduction of service), requests for information (including how-to instructions), and requests for HPC services. The Contractor's standard Service Desk support includes, but is not limited to, the following requirements:

- The Contractor shall support HPC Service Desk during NETL Business Operating Hours described in the Section 1 – Introduction.
- The Contractor shall provide HPC Service Desk Responsibility. The Contractor shall provide courteous, prompt, high-quality end user support services, including RSA Token delivery to HPC users. Both the appropriate level of technical expertise and the presence of professional demeanor shall define the Contractor's end user support personnel. The Contractor shall respond (either by phone call or email) to the customer within 1 business day of a customer's request. The Contractor shall resolve the request within 1-3 days (or longer with documentation and weekly customer updates).
- The Contractor shall provide HPC Service Desk Email/Phone Service. The Contractor shall be available to support employees through a single email address and phone number.
- The Contractor shall support the HPC Vetting Process. The Contractor shall maintain and track user documents for the HPC-specific vetting process such as user information, directorate, Field Work Proposal (FWP), the needed hardware and software resources, and agreements including Computer Account Security Agreement (CASA).
- The Contractor shall maintain and track all HPC service desk tickets, maintaining workflow status information for accuracy and currency to make the information—such as description of the fix action, estimated time of completion, and responsible point of contact—available to HPC customers.
- The Contractor shall provide HPC Outage/Incident Notification. The Contractor shall provide timely notifications to users and appropriate Government points of contact of planned (with prior Government approval) and unplanned outages/incidents of systems, networks, and other major components using Government approved communication methods.
- The Contractor shall provide End User Training. The Contractor shall support the training required for HPC users such as new employees and summer interns. This support may deliver training materials, including, but not limited to presentations and learning aids for online, classroom, and informal brown bag style sessions.
- The Contractor shall support Website Development. The Contractor shall perform website design and development for the HPC. The Contractor shall provide editorial support for web content and ensure that all websites and content are up-to-date for Joule and Watt.

5.3.4.6 HPC Service Purchasing Support

The Contractor shall assist in the procurement of the HPC and Data Center, as well as Procurement Support laid out in the Section 2 – General Contract Requirements. The Contractor shall provide HPC Service Purchasing Support for products, materials, services, and Other Direct Cost (ODC) in support of HPC activities. This will require the Contractor to implement an efficient procurement management process with the capability to support. The objective is to provide purchasing and billing support in such a manner as to maintain a secure and modern HPC and Data Center through proper hardware/software/material upgrades, refreshes, and renewals. Specific requirements include but are not limited to:

- The Contractor shall perform HPC and Data Center market surveys and prepare input for purchase requests per DOE/NETL federal acquisition regulations, shall obtain cost estimates, and shall track the purchase(s) through to completion, including receipt and inventory management. The Contractor shall provide a comprehensive supply chain management plan which will ensure the quality, availability, and security of all resources.

- The Contractor shall procure items as approved through the annual planning and budget approval process to maintain the HPC and Data Center hosting HPC.
- The Contractor's processes and procedures will ensure the selection of competent suppliers, recommend unbiased purchase decisions, establish compliant contracts, and negotiate competitive prices for goods and services as authorized by the Government in a cost-effective manner and in accordance with public law and applicable regulations.

5.3.5 Performance Expectations/Inspection and Acceptance

Performance Objective	Performance Expectation	Surveillance Method
HPC services are available to the research user community.	Adherence to the response guidelines > 98% of the time.	NETL shall assess the degree to which adherence to the response guidelines is followed through service interruption documentation and customer complaints.
All HPC equipment and services are protected appropriately from threats (particularly cyber threats).	99% of all HPC data center systems and services are scanned, patched, and updated within two weeks of patch release, unless superseded by government mandates, without negative impact to the users. <2% of all other HPC patches and upgrades have a negative impact on users.	NETL shall assess the degree to which HPC equipment is protected appropriately through cyber scans and other threat management detection methods.
HPC User support is provided in an effective, courteous, and timely manner.	>90% of customers report on surveys a satisfactory or higher rating when dealing with user support services. >90% of all service requests are resolved and closed within an appropriate amount of time.	NETL shall assess the degree to which user support is effective and courteous through customer surveys and validated customer complaints. NETL shall assess the degree to which the user support is timely through periodic review of the monthly activity reports and periodic audits of the incident tracking system.
All HPC documentation (including configuration information) is maintained appropriately.	99% of all documentation required to manage the HPC is complete and current.	NETL shall assess the degree to which the HPC documentation is maintained appropriately through periodic audits.
Changes to the HPC are managed consistently through the change management process to avoid possible negative impacts to HPC equipment and services.	100% of all changes are done through the change management process.	NETL shall assess the degree to which adherence to the change management process is followed consistently through review of monthly activity reports, change management records, and periodic audits.
HPC assets (hardware and software) are managed and tracked appropriately.	100% of license/agreement renewals are completed before expiration date. 100% of all assets are tracked.	NETL shall assess the degree to which the HPC assets are tracked and managed appropriately through review of monthly activity reports and

		periodic review of database reports.
HPC risks are managed appropriately so that HPC services to users are not impacted.	>95% of the time, proactively identify risks prior to them becoming issues , and remediations/improvements are suggested prior to failure.	NETL shall assess the degree to which HPC risks are managed appropriately through review of the monthly activity reports and periodic audits.

5.3.6 Deliverables/Schedule

HPC Annual Disaster Recovery Plan (DRP) – The Contractor shall develop and test a DRP within the first twelve months of the contract, maintain up-to-date plans to ensure changes in the HPC environment and evolving technologies implemented at NETL are considered and addressed, and test annually a DRP for the HPC systems, network, applications, and services which are well-structured and easily understood, and which will aid NETL in the recovery of business operations as quickly and effectively as possible from an unforeseen disaster or event. The DRP shall include step-by-step recovery instructions for restoring the HPC facilities, systems, networks, applications, and services and be stored in a secure offsite location.

Service Interruption Report (SIR) – The Contractor shall submit an SIR for every HPC service outage or significant degradation within five days of the event. The SIR shall include detailed event information, findings, remediation activities, and lessons learned. (Typically, there are less than 10 of these a year.)

As-Built Documentation – The Contractor shall provide documentation for new HPC systems/applications/services within five days of the systems/application/service being released into the production environment.

Monthly Activity Report (MAR) and **Monthly Cost Management Report (CMR**) – The Contractor shall provide a monthly report of the HPC activities and progress including but not limited to current HPC initiatives/status, discussion of any deviations from the planned work for the report period, projected schedule and resource requirement estimate for the current month's planned activities, uptime, outages, service interruption reports, problems, and corrective actions for all HPC services and systems, highlights of monthly activities for the HPC Service Desk, summary of all purchase requests submitted, and purchases received.

HPC Semi-Annual Preventative Maintenance Plan and Schedule – The Contractor shall provide a recommended HPC semi-annual preventative maintenance plan and schedule at the start of each new contract year, developed, and implemented in a manner consistent with industry standards and guidelines and manufacturer-recommended maintenance schedules.

HPC Quarterly Energy Audit Report – The Contractor shall provide a quarterly report of the energy usage of all HPC systems and Data Center.

HPC Quarterly Data Call Response – The Contractor shall support Quarterly HPC Data Calls about Budget: Current Year (Q1-Q4) Planned/Obligated/Actuals Budget information and the estimated budget for the next 4 years (Lifecycle cost).

HPC Weekly Status Report – The Contractor shall provide a weekly report of the status of all HPC systems, including but not limited to, hardware maintenance list, open issues, and lifecycle status, HPC infrastructure operations and service operations status, and patch status.

5.4 Activity 00005b – Energy Data Exchange (EDX)

5.4.1 Activity Type

This Activity is cost-plus award fee.

5.4.2 Place of Performance

For specific operations and maintenance actions requiring hands-on work or face-to-face, direct stakeholder interaction, the place of performance for this CLIN is at NETL sites located in Albany, OR, Morgantown, WV, and Pittsburgh, PA. The Energy Data Exchange (EDX) hardware is primarily located in Morgantown, WV.

5.4.3 Objective

The objective of this Activity is to provide IT support for all aspects of NETL's EDX and its research data management.

5.4.4 Background/Introduction

EDX is an NETL-hosted external custom web-based data library and virtual scientific computing laboratory tool for the Department of Energy's (DOE) Fossil Energy and Carbon Management (https://edx.netl.doe.gov/). Developed by NETL's Research & Innovation Center (R&IC), EDX includes elements of data warehouses and portals combined with advanced online scientific computing solutions, tools, and analytical capabilities pertinent to ensuring efficient and timely execution of and dissemination of energy research-related needs as part of NETL and DOE's energy research and development (R&D) mission. EDX's website contains an "about" page for more information (https://edx.netl.doe.gov/about). EDX includes a public-facing half as well as a private secure-based half, both of which are web-based.

Being a web-based system, the hours of operation are 24 hours a day, 7 days a week, 365 days a year. In addition to requiring continuity of operations without disruption, because EDX is public-facing, EDX is increasingly being utilized by DOE headquarters and other DOE National Laboratories to support ongoing research needs as well as Executive and DOE orders related to ensuring the preservation and accessibility to federally funded R&D products. In FY15, EDX was adopted by the DOE Subsurface R&D Crosscut as one of two systems for data sharing and preservation for the DOE-wide effort.

EDX IT Support encompasses all the functions and services which are needed for support of the NETL EDX environment, including but not limited to, hardware and software support, data and application services, cloud services, the communications between individuals and services, and first contact support for those users. There are two distinct pieces to EDX IT support: 1) standard operations and maintenance (O&M) and 2) research tools development and support.

- The O&M work is expected to be consistent from year-to-year and may include development work on the EDX system. EDX releases monthly system updates as a result of the O&M development work.
- The research development and support work are based on approved research projects, will vary each year, and always involves milestones. Hereafter, the research tools development and support will be referred to as "dev-tasks."

Contractor resources in this effort shall coordinate and interact with other IT personnel and resources in conformance with NETL policies, protocols, and cybersecurity requirements.

5.4.5 Scope/Requirements

Direction Regarding General Contract Requirements

The Contractor shall perform all work within this Activity according to the requirements specified in the General Contract Requirements section.

- **Risk Management:** In addition to the requirements provided in the General Contract Requirements for Risk Management *[2.1.3]*, the Contractor shall specifically be responsible for identifying risks to the functionality of the EDX and submitting and managing risks in the risk register in accordance with the risk management process.
- **Change Management:** In addition to the requirements provided in the General Contract Requirements for Change Management *[2.1.4]*, the Contractor shall specifically be responsible for consulting with others to determine the impact of a proposed change on NETL's environment and preparing, submitting, and implementing change requests in accordance with the change management process.
- **Configuration Management:** In addition to the requirements provided in the General Contract Requirements for Configuration Management *[2.1.5],* the Contractor shall specifically be responsible for maintaining the underlying EDX code and any explanatory and supporting documentation in a coherent and complete manner.
- **Knowledge Management:** In addition to the requirements provided in the General Contract Requirements for Knowledge Management *2.1.6]*, the Contractor shall specifically be responsible for preparing and maintaining any operational drawings, architecture drawings, and diagrams which facilitate the documentation and understanding of the EDX processes and/or systems.
- **IT Asset Management:** In addition to the requirements provided in the General Contract Requirements for IT Asset Management *[2.1.10]*, the Contractor shall specifically be responsible for managing certain EDX hardware and software licenses and agreements in a manner which maintains the provision of the EDX services to its customers. The support requirements include, but are not limited to:
  - Manage maintenance/service agreements.
  - Track all maintenance/service agreement periods, notify the TCOR of any that will expire in 90 or fewer calendar days, and submit purchase requisition(s) to the Government procurement system for renewal at least 60 calendar days prior to the expiration date.
  - Coordinate maintenance/repair provided by external providers, including site visits and returns for repairs.
  - Manage software licenses.
  - Track license periods, notify the TCOR of any that will expire in 90 or fewer calendar days, and submit purchase requisition(s) to the Government procurement system for renewal at least 60 calendar days prior to the expiration date.
  - Track license distributions.
  - Ensure adequate license coverage and inform the TCOR when license levels are in jeopardy of being exhausted.
  - Retire and dispose of excess license materials in conjunction with the Government property management function.

Data Center Support

While data centers are primarily managed by Enterprise Infrastructure *[CLIN 00002]*, it is expected that the Contractor will clearly define requirements and work with Enterprise Infrastructure *[CLIN 00002]* personnel to manage EDX's hardware and connections within NETL's data centers while meeting all policies, protocols, standards, and requirements as specified by Enterprise Infrastructure *[CLIN 00002]*and government mandates. Inherent in this requirement is any work associated with moving on-premises hardware to a new location as required.

Networks Support

While networks are primarily managed by Enterprise Infrastructure *[CLIN 00002]*the Contractor shall clearly define requirements and work with Enterprise Infrastructure *[CLIN 00002]* personnel to manage EDX's hardware and connections while meeting all policies, protocols, standards, and requirements as specified by Enterprise Infrastructure *[CLIN 00002]*and government mandates.

Hours of Operation and Support

Being a web-based system, the hours of operation are 24 hours a day, 7 days a week, 365 days a year, even during site closings for weather.

- During NETL Business Hours, it is expected that the loss of EDX services shall result in immediate (within 15 minutes) response times for remediation.
- Outside of NETL Business Hours, it is expected that the Contractor shall respond within 60 minutes, and if necessary to restore service per Government direction, have staff on-site within three hours of initial contact to troubleshoot and resolve the service interruption or identified problem.

It is preferred that all updates and maintenance be performed outside of NETL Business Hours in coordination with the change management process.

EDX Infrastructure Management

The Contractor shall provide all support required to design, procure, deploy, maintain, and refresh/upgrade all EDX infrastructure equipment. This equipment includes, but is not limited to, servers, switches, and data storage.

The Contractor shall provide all associated services with maintaining the functionality of the EDX infrastructure including, but not limited to, backup and recovery management of all EDX data and configurations, database management, networked software license management, remote connection management, and cloud services management.

The Contractor shall integrate any new system or tool properly into the EDX.

The Contractor shall provide data manipulation necessary to format raw data for EDX tool processing.

The Contractor shall provide preventive maintenance activities for the EDX infrastructure. All preventative maintenance activities shall be performed without negatively impacting the user community. This preventative maintenance includes, but is not limited to, patching, updates, and version control on EDX systems and servers according to established timelines.

The Contractor shall continuously monitor—to the extent possible—the health, security, availability, and performance of all EDX systems.

The Contractor shall provide infrastructure planning support in such a manner as to improve and develop the EDX over the long term.

Cloud Services Support

EDX is being directed to integrate across an array of cloud services and is currently evaluating various possibilities for use in research and analytics. Hybrid solutions—both on-premises and in the cloud—are anticipated. The support requirements include, but are not limited to:

- Provide an experienced, working knowledge of cloud services, architecture, and interactions for analysis and for EDX platform curation.
- Understand how information is managed, the cybersecurity ramifications of various options, the costs involved, and ways to optimize so that appropriate choices can be made to expand the EDX system properly into the cloud.
- Make recommendations on future directions and opportunities to evolve.
- Manage any cloud system that becomes part of the EDX system.
- Provide cloud cybersecurity experience for work which could include ATO/ATU support, system-level security and privacy policies and controls development, or other cyber-related

milestones which must be achieved to successfully support EDX. Cloud Security experience is seen as essential to enabling proper cloud design and selection which meets cyber mandates (e.g., NIST RMF, FedRAMP ATO process, System Security Plan development, etc.) as well as research requirements.

Work Management

The Contractor shall manage the dev-tasks in concert with the O&M work in a manner which results in achieving the defined technical, cost, and schedule objectives and milestones. The support requirements include, but are not limited to:

- Provide accurate and timely status reports.
- Determine and communicate the impact of a change on one dev-task to all other active or planned dev-tasks.
- Manage critical paths, coordinate key integration points, and develop contingencies to deal with the risk and uncertainty inherent in IT projects.
- Manage and run the weekly EDX Operations and Development Coordination Meeting (currently held every Tuesday at noon EST).

User Support

The Contractor shall provide technically knowledgeable, courteous, and responsive first-contact support to user requests for assistance. Since EDX does not deploy or manage endpoints, this primarily refers to requests for EDX services (user access/accounts), requests for information (including how-to instructions) regarding usage of EDX website and tools, and notifications of service interruptions or issues. This support is expected to be available during NETL Business Hours.

As EDX users include both NETL employees and non-NETL employees, support is available both through the Government-provided tool and through a separate email and phone number. The Contractor shall maintain and monitor all of these existing methods of communication.

The Contractor shall utilize the Government-provided tool to document all service requests (including those made to the separate emails/phone numbers) and to maintain a knowledge database of solutions.

The Contractor shall respond (either by phone call or email) to the customer within 1 business day of a customer's request. The Contractor shall resolve the request within 1-3 days (or longer with documentation and weekly customer updates).

Design and Engineering Support

The Contractor shall provide design and engineering support in such a manner as to maintain a modern EDX through appropriate design choices, proper upgrades, and timely refreshes. This support shall include all IT devices required to support the functionality of EDX except for those specifically under the management of a different entity or CLIN. Inherent in this support is the collaboration—and standardization where possible—across the NETL IT infrastructure and participation in any architectural reviews. All designs—from on-premises servers to internet to cloud—should fit into the overall EDX plan. Some specific support requirements include, but are not limited to:

- Provide cutting-edge code development, communications, and data management approaches in support of EDX goals.
- Provide engineering and technical expertise to aid the development of technical requirements packages to support authorized IT-related purchases (e.g., equipment, software, maintenance agreements, licenses, etc.).

5.4.6 Performance Expectations/Inspection and Acceptance

The performance expectations for the EDX Activity are summarized into performance objectives listed below followed by the performance expectation and the surveillance method. The performance expectation is the standard for which services will be accepted.

Performance Objective	Performance Expectation	Surveillance Method
EDX services are available to the research user community.	Adherence to the response guidelines > 98% of the time.	NETL shall assess the degree to which adherence to the response guidelines is followed through service interruption documentation and customer complaints.
All EDX equipment and services are protected appropriately from threats (particularly cyber threats).	99% of all EDX systems and services are scanned, patched, and updated within two weeks of patch release, unless superseded by government mandates, without negative impact to the users.	NETL shall assess the degree to which EDX equipment is protected appropriately through cyber scans and other threat management detection methods.
User support is provided in an effective, courteous, and timely manner.	>90% of customers report on surveys a satisfactory or higher rating when dealing with user support services. >90% of all service requests are resolved and closed within the time specified in the Government-provided tool that documents all service requests.	NETL shall assess the degree to which user support is effective and courteous through customer surveys and validated customer complaints. NETL shall assess the degree to which the user support is timely through periodic review of the monthly activity reports and periodic audits of the incident tracking system.
All EDX documentation (including configuration information) is maintained appropriately.	99% of all documentation required to manage EDX is complete and current.	NETL shall assess the degree to which the EDX documentation is maintained appropriately through periodic audits.
Changes to EDX are managed consistently through the change management process to avoid possible negative impacts to EDX equipment and services.	100% of all changes are done through the change management process.	NETL shall assess the degree to which adherence to the change management process is followed consistently through review of monthly activity reports, change management records, and periodic audits.
EDX assets (hardware and software) are managed and tracked appropriately.	100% of license/agreement renewals are completed before expiration date. 100% of all assets are tracked.	NETL shall assess the degree to which the EDX assets are tracked and managed appropriately through review of monthly activity reports and periodic review of database reports.
EDX risks are managed appropriately so that EDX services to users are not impacted.	>95% of the time, proactively identify risks prior to them becoming issues, and remediations/improvements are suggested prior to failure.	NETL shall assess the degree to which EDX risks are managed appropriately through review of the monthly activity reports and periodic audits.

5.4.7 Deliverables/Schedule

EDX Annual Disaster Recovery Plan (DRP) – The Contractor shall develop (within the first 12 months of the contract start), maintain (i.e., keep updated with EDX changes), and test (after development and each contract year) a DRP for the EDX systems and services, including the computer facilities and systems and the communications systems with documented federal approval. The DRP shall include step-by-step recovery instructions and be stored in a secure offsite location.

EDX Annual Preventative Maintenance Plan and Schedule – The Contractor shall provide a recommended EDX annual preventative maintenance plan and schedule 60 days after the start of the contract and at the start of each new contract year, developed and implemented in a manner consistent with industry standards and guidelines and manufacturer-recommended maintenance schedules.

As-Built Documentation – The Contractor shall provide documentation for new applications/services/tools within five days of the application/service/tool being released into the IT production environment.

EDX Quarterly Status Report – The Contractor shall provide a quarterly report of the status of all EDX systems and services.

Service Interruption Report (SIR) – The Contractor shall submit a SIR for every EDX service outage or significant degradation within five days of the event. The SIR shall include detailed event information, findings, remediation activities, and lessons learned. (Typically, there are less than 10 of these a year.)

6 CLIN 00006 – Operations and Maintenance Actions Indefinite Delivery-Indefinite Quantity (IDIQ) – Firm-Fixed Price IDIQ

6.1 CLIN Type

This CLIN is planned to be firm-fixed price.

6.2 Place of Performance

For specific operations and maintenance actions requiring hands-on work or face-to-face, direct stakeholder interaction, the place of performance for this CLIN is at NETL Albany, OR, Morgantown, WV, and Pittsburgh, PA sites.

6.3 Objectives

TBD

6.4 Scope /Requirements

TBD

6.5 Performance Expectations/Inspection and Acceptance

TBD

6.6 Deliverables/Schedule

TBD

6.7 Resource Load Information

TBD

7 CLIN 00007 – Operations and Maintenance Actions Indefinite Delivery-Indefinite Quantity (IDIQ) – Cost-Plus-Award-Fee IDIQ

7.1 CLIN Type

This CLIN is planned to be cost-plus-fixed-fee.

7.2 Place of Performance

For specific operations and maintenance actions requiring hands-on work or face-to-face, direct stakeholder interaction, the place of performance for this CLIN is at NETL Albany, OR, Morgantown, WV, and Pittsburgh, PA sites.

7.3 Objectives

TBD

7.4 Scope /Requirements

TBD

7.5 Performance Expectations/Inspection and Acceptance

TBD

7.6 Deliverables/Schedule

TBD

7.7 Resource Load Information

TBD

8 CLIN 00008 – Transition

8.1 CLIN Type

This CLIN is cost-no fee.

8.2 Place of Performance

For specific operations and maintenance actions requiring hands-on work or face-to-face, direct stakeholder interaction, the place of performance for this CLIN is at NETL Albany, OR, Morgantown, WV, and Pittsburgh, PA sites.

8.3 Objectives

Transition services are comprised of all transition activities to begin performance of ITSS2, consistent with this contract. Transition activities are defined as any effort which is necessary to transition the work from the incumbent Contractor in a manner that (1) ensures that all work for which the Contractor is responsible under the contract is continued without disruption; (2) provides for an orderly transfer of resources, responsibilities, and accountability from the incumbent Contractor; and (3) allows the Contractor to perform the work in an efficient, effective, and safe manner. The specific transition activities are to be included in a Transition Plan, the contents of which are identified in Section L of the solicitation. The Transition Plan submitted with the proposal will be the starting point for a finalized plan.

In accordance with the solicitation and contract, transition is not fee bearing. Transition functions align with the FAR 52.237-3 Continuity of Services clauses of the predecessor contracts and should be planned for the orderly and efficient transition of work from the predecessor contracts to the successor. Work under this CLIN covers actions required to transfer work from the current Information Technology Site Support (ITSS) contract, (the incumbents) to newly awarded ITSS2. The Contractor is expected to complete the orderly, efficient, and effective transition of work to assume full work requirements within the transition period.

8.3.1 Scope /Requirements

The Contractor shall implement all transition activities to begin performance of the ITSS2, consistent with the Transition Plan and Milestone Schedule as submitted in response to the solicitation, finalized and approved during the kickoff meeting.

The Contractor shall provide a seamless transfer of responsibility for ongoing and new work assignments during the transition period:

- Uninterrupted delivery of activity assignments.
    - The Contractor shall conduct knowledge transfer to capture and retain existing knowledge that provides for an orderly transfer of resources, responsibilities, and accountability from the incumbent Contractor.
- Sustained, high quality execution of assignments.
    - The Contractor shall review NETL SOPs to ensure a complete understanding of current processes, workflow, infrastructure, business, and technical complexity.
    - The Contractor shall review NETL's IT Governance structures, to include the IT Project Management process, the IT Architecture Board, the Risk Review Board, and the Change Control Board, to ensure a complete understanding of Governance processes.
    - The Contractor shall review all in-process IT projects with the incumbent in order to seamlessly transfer performance responsibility.
    - The Contractor shall work with federal staff and other Contractors as required to accomplish requirements, goals, and objectives as efficiently and effectively as possible. This will likely include sharing information resulting from the work required by this Performance Work Statement (PWS) or previous Government efforts with the objective of gaining a clear operational understanding of the body of work to be performed.
- Government Property responsibilities.
    - Accountable and sensitive property currently issued to the incumbent Contractor for contract performance will be provided to the Contractor for performance of activities under this contract. During the transition period, a wall-to-wall physical inventory shall be completed and an acceptance of the full accountable and sensitive property at the end of transition.
    - A copy of the Contractor's property management systems procedures shall be provided for review and concurrence to the Government Property Administrator.

8.3.2 Deliverables/Schedule

- During transition, deliverables shall be provided in accordance with the Reporting Requirements Checklist.
- Transition shall be complete within the transition period.

8.3.3 Resource Load Information

- The Contractor shall review the historical information identified in the solicitation and the minimum qualifications as identified in Section J, Attachment C – Position Qualifications of the contract for the type and number of staffing historically utilized.
- The Contractor shall contract for, interview, and hire qualified staff to successfully perform the activities defined in this PWS within the duration of the transition period.
- The Contractor shall establish market appropriate employee relations at the point of transition, including addressing employee benefits, and employee concerns; and avoiding disruption of service during transition.
- During the kick-off meeting, NETL will coordinate with the incumbent to provide the successful offeror a list of incumbent names, including email addresses, and labor categories.
- Human Resource functions which are required shall be done off-site and after hours. NETL will allow the use of intranet postings to post "Job Fair" announcements associated with the transition.

9 Appendix

9.1 Acronyms

A&A	Assessment and Authorization
ADFS	Active Directory Federation Services
ALB	Albany National Energy Technology Laboratory Site
AI	Artificial Intelligence
AO	Authorizing Official
AODR	Authorizing Official Designated Representative
ATO	Authority to Operate
ATU	Authority to Use
A/V	Audio/Visual
BIA	Business Impact Analysis
BOD	Binding Operational Directive
BYOD	Bring Your Own Device
C&A	Certification and Accreditation
CAB	Change Advisory Board
CAML	Center for Artificial Intelligence and Machine Learning
CD	Critical Decision
CI	Configuration Item
CIO	Chief Information Officer
CLIN	Contract Line-Item Number
CMDB	Configuration Management Database
CMMI	Capability Maturity Model Integration
CMR	Cost Management Report
CO	Contracting Officer
COO	Chief Operating Officer
COR	Contracting Officer Recognition
COTS	Commercial Off the Shelf
CPU	Central Processing Unit
CSE	Computational Science and Engineering Center
CSP	Cloud Service Provider
DCOI	Data Center Optimization Initiative
DFAS	Defense Finance and Accounting Service
DHCP	Dynamic Host Configuration Protocol
DHS	Department of Homeland Security
DIMM	Dual In-Line Memory Module
DL	Deep Learning
DMBOK	Data Management Body of Knowledge
DMZ	Demilitarized Zone
DNS	Domain Name Services
DOE	Department of Energy

DOE HQ	Department of Energy, Headquarters
DOE PEM	Department of Energy Project Execution Model
DRP	Disaster Recovery Plan
EDX	Energy Data Exchange
EOL	End of Life
EOS	End of Support
ESNET	Energy Sciences Network
EST	Eastern Standard Time
FAR	Federal Acquisition Regulations
FE	Fossil Energy
FECM	Fossil Energy Carbon Management
FedRamp	Federal Risk and Authorization Management Program
FISMA	Federal Information Security Management Act
FITARA	Federal Information Technology Act
GETS	Government Emergency Telecommunications Services
GFE	Government Furnished Equipment
GPOs	Government Policy Objects
GPRA	Government Performance and Results Act
GPU	Graphics Processing Unit
GSA	General Service Administration
HDD	Hard Disk Drive
HPC	High Performance Computing
HTTP/HTTPS	Hypertext transfer Protocol Secure
IaaS	Infrastructure as a Service
ICDS	Interface Control Documents
ICS	Industrial Control Systems
IDIQ	Indefinite Delivery Indefinite Quantity
IPAM	Internet Protocol Address Management
IPMI	Intelligent Platform Management Interface
IPS/IDP	Intrusion Prevention and Detection Services
ISE	Identity Service Engine
ISO	International Standards Organization
IT	Information Technology
ITAB	Information Technology Architecture Board
ITARB	Information Technology Review Board
ITIL	Information Technology Infrastructure Library
ITSM	Information Technology Service Management
ITSS2	Information Technology Support Services
KEDB	Known Error Database
KM	Knowledge Management
LAN	Local Area Network
LMR	Land Mobile Radio
MAR	Monthly Activity Reports

MDC	Modular Data Center
MDM	Mobile Device Management
MFA	Multi Factor Authentication
MGN	Morgantown National Energy Technology Laboratory Site
ML	Machine Learning
MPLS	Multiprotocol Label Switching
NAC	Cisco Identity Services Engine Network
NARA	National Archives and Record Administration
NETL	National Energy Technology Laboratory
NFS	Network File System
NNSS	Nevada National Security Site
NIST	National Institute of Standards and Technology
NTIA	National Telecommunications & Information Administration
NTP	Network Time Protocol
NVME	Non-Volatile Memory Express
O&M	Operations and Maintenance
OLC2	DOE's Online Learning Center
OLTP	Online Transaction Processing
OMB	Office of Management and Budget
OPM	US Office of Personnel Management
OSSA	Operating System Security Assessment
PaaS	Platform as a Service
PC	Personal Computer
PDB	Power Distribution Board
PEM	Project Execution Manual
PGH	Pittsburgh National Energy Technology Laboratory Site
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
PLC	Programmable Logic Controller
PMP	Project Management Plan
POAM	Plans of Actions and Milestones
PSTN	Public Switched Telephone Network
PTS	Personnel Tracking System
PWS	Performance Work Statement
QAMP	Quality Assurance Management Plan
QOS	Quality of Service
RAM	Random Access Memory
R&D	Research & Development
R&IC	Research & Innovation Center
RelMF	Release Management Framework
ReqMF	Requirements Management Framework
RMF	Risk Management Framework

ROM	Rough Order of Magnitude
RVA	Risk Vulnerability Assessment
SaaS	Software as a Service
SAS	Serial Attached SCSI
SAV	Site Assistance Visit
Science Lan	Science Local Area Network
SDLC	Standard Systems Development and Lifecycle Management
SLA	Service Level Agreement
SIP	Session Initiation Protocol
SIR	Service Interruption Report
SME	Subject Matter Expert
SOE	Standard Operating Equipment
SOPs	Standard Operating Procedures
SPAN	Switch Port Analyzer
SQA	Software Quality Assurance
SQL	Structured Query Language
SSH	Secured Shell
STARS	Standard Accounting and Reporting System
STRIPES	Strategic Integration Procurement Enterprise System
TIC	Trusted Internet Connection
TICAP	Trusted Internet Connection Access Point
TMF	Test Management Framework
TSP	Telecomm Service Priority
UAT	User Acceptance Testing
UC	Unified Communications
VDI	Virtual Desktop Infrastructure
VHF	Very High Frequency
VIP	Very Important Person
VLAN	Virtual Local Area Network
VOIP	Voice Over Internet Protocol
VTC	Video Teleconferencing
WAN	Wide Area Network
WLAN	Wireless Local Area Network
WSE	Wafer-Scale Engine
WPS	Wireless Priority Services
ZTA	Zero Trust Architecture