Statement of Work

Enterprise Facility Infrastructure Engineering and Operations Support for BARC, BHNRC, and USNA During BARC Transition and Closure

1.0 Background

Personnel and operational activities at the U.S. National Arboretum (USNA) are increasing as functions are relocated from the Beltsville Agricultural Research Center (BARC), creating greater demand on shared network, compute, storage, database, monitoring, cybersecurity, and facility-supporting infrastructure. At the same time, BARC research programs, scientific data, applications, and supporting systems are being transferred to receiving locations throughout the United States, requiring the existing infrastructure to remain secure, reliable, and continuously available throughout the migration process.

The United States Department of Agriculture (USDA) Agricultural Research Service (ARS) relies on BARC, the Beltsville Human Nutrition Research Center (BHNRC), and USNA to conduct mission-critical research and support laboratory operations, facility systems, environmental monitoring, cybersecurity, and administrative functions. These locations operate through an interconnected enterprise infrastructure that provides shared services essential to daily Government operations.

USDA requires enterprise infrastructure operations and engineering support to sustain mission-critical IT services across BARC, BHNRC, and USNA during the ongoing BARC transition and phased closure. The contractor must support current operations while enabling the orderly migration of research workloads, scientific data, applications, and associated systems to their receiving locations. This includes maintaining source systems, protecting data integrity, identifying technical dependencies, supporting secure transfers and cutovers, and validating that migrated services operate successfully at their destinations.

This requirement provides the operations, engineering, maintenance, migration support, and technical expertise necessary to maintain system availability, address cybersecurity vulnerabilities, manage infrastructure capacity and lifecycle requirements, and preserve continuity of Government operations. These services support laboratory safety systems, facility access controls, environmental monitoring, research computing, bioinformatics processing, scientific databases, and administrative functions while maintaining compliance with FISMA, NIST SP 800-53, USDA cybersecurity policies, and other applicable federal requirements.

2.0 Scope of Work

This requirement provides enterprise infrastructure operations and engineering support necessary to maintain the availability, security, reliability, and performance of mission-critical IT services supporting the Beltsville Agricultural Research Center (BARC), Beltsville Human Nutrition Research Center (BHNRC), and U.S. National Arboretum (USNA). The Contractor shall provide Tier II and Tier III operations and engineering support for enterprise network, virtualization, database, application, storage, monitoring, patch management, and facility-supporting infrastructure that enables mission operations, enterprise services, environmental monitoring, security systems, facility operations, and administrative functions.

The Contractor shall maintain continuity of operations across interconnected enterprise environments while supporting the ongoing BARC transition and phased closure. Services shall include infrastructure operations, systems engineering, capacity planning, lifecycle management, technology refresh, performance optimization, cybersecurity, operational monitoring, and technical support necessary to ensure the continued availability, resilience, and security of mission-critical Government services.

The Contractor shall also provide engineering support to facilitate the orderly relocation of mission functions, personnel, enterprise applications, data, and supporting infrastructure to receiving USDA locations throughout the United States. This includes maintaining source environments, identifying technical dependencies, coordinating infrastructure changes and technical cutovers, supporting data migration activities, validating operational readiness, and minimizing disruption to Government operations throughout the transition.

Because the enterprise infrastructure supporting BARC, BHNRC, and USNA remains operationally integrated, and because personnel and operational activities continue to increase at USNA, the Contractor shall ensure the infrastructure can support evolving mission requirements while maintaining system availability, protecting data integrity, preserving cybersecurity compliance, and minimizing operational risk.

All work performed under this contract shall comply with applicable federal cybersecurity and information protection requirements, including FISMA (44 U.S.C. § 3551 et seq.), NIST SP 800-53, USDA Departmental Manual 3515-001, and other applicable USDA policies.

2.1 Enterprise Network Operations and Engineering Support

The Contractor shall provide enterprise network operations and engineering support necessary to sustain the USDA Agricultural Research Service Northeast Area Brocade (Ruckus) network infrastructure supporting BARC, BHNRC, USNA, and associated interconnected enterprise environments. The network provides mission-critical connectivity for administrative operations, cybersecurity services, facility access controls, environmental monitoring systems, safety- and health-related functions, and shared enterprise services supporting ongoing Government operations.

Support activities shall include network administration, operational monitoring, performance analysis, configuration management, firmware and software lifecycle management, vulnerability remediation, incident response, advanced troubleshooting, capacity planning, network optimization, and manufacturer warranty and replacement coordination for Brocade (Ruckus) switching infrastructure and associated enterprise network components.

The Contractor shall provide engineering support necessary to maintain and adapt the Northeast Area enterprise network as mission requirements evolve during the BARC transition and phased closure. Engineering activities shall include evaluating network utilization and capacity, supporting infrastructure expansion, planning and implementing network modifications, validating connectivity for relocated personnel, systems, and operational functions, recommending technology refresh solutions, and ensuring secure, resilient, and scalable network services across supported Northeast Area environments.

All network operations, maintenance, replacement, and engineering activities shall be coordinated to maintain system availability, minimize operational risk, preserve existing dependencies, and avoid disruption to mission-critical Government services. Work performed under this task shall comply with FISMA, NIST SP 800-53, USDA Departmental Manual 3515-001, and other applicable USDA cybersecurity and information protection requirements.

2.2 Enterprise Virtualization Operations and Engineering Support

The Contractor shall provide engineering and operational support to maintain, optimize, and enhance the USDA Agricultural Research Service (ARS) Northeast Area enterprise virtualization environment as mission requirements evolve during the BARC transition and phased closure. Engineering activities shall include provisioning and decommissioning virtual resources, supporting infrastructure modifications,

optimizing compute capacity, implementing technology refresh and performance improvements, and validating application and system performance to maintain a secure, scalable, resilient, and highly available enterprise virtualization environment.

The Contractor shall provide operations and lifecycle management for the enterprise virtualization infrastructure supporting BARC, BHNRC, USNA, and associated enterprise environments. Services shall include virtualization platform administration, virtual machine lifecycle management, configuration management, performance monitoring, capacity planning, patch management, vulnerability remediation, backup integration, disaster recovery support, advanced troubleshooting, and infrastructure optimization to ensure continuous availability and operational resilience.

The Contractor shall also support the preparation, migration, validation, and decommissioning of virtual workloads associated with the relocation of ARS mission functions, personnel, applications, and supporting systems to receiving locations throughout the United States. This includes maintaining source environments, coordinating technical cutovers, validating operational readiness following migration, and minimizing service disruption while preserving continuity of Government operations.

All virtualization operations and engineering activities shall be coordinated to maintain system availability, protect data integrity, minimize operational risk, and ensure compliance with FISMA, NIST SP 800-53, USDA Departmental Manual 3515-001, and other applicable USDA cybersecurity and information protection requirements.

2.3 Enterprise Facility Infrastructure Engineering and Operations Support

As personnel, mission functions, and operational activities continue to increase at the U.S. National Arboretum (USNA) during the BARC transition and phased closure, the Contractor shall provide enterprise facility infrastructure engineering and operations support necessary to expand, adapt, and sustain the IT infrastructure supporting evolving Government mission requirements. This includes the engineering and operational support required for enterprise computing facilities, telecommunications infrastructure, structured cabling, equipment installations, power distribution, environmental controls, equipment relocation, and other IT facility components essential to maintaining mission-critical Government operations.

The Contractor shall provide engineering support to assess, design, implement, and optimize facility infrastructure necessary to accommodate changing operational requirements across the USDA Agricultural Research Service (ARS) Northeast Area (NEA). Engineering activities shall include infrastructure assessments, equipment installation and relocation planning, rack and cabinet engineering, structured cabling design and coordination, power and cooling capacity analysis, telecommunications infrastructure expansion, equipment decommissioning, technology refresh planning, and facility infrastructure modifications required to support the continued growth of USNA and the orderly transition of mission functions from BARC.

The Contractor shall evaluate existing facility infrastructure capacity and recommend enhancements necessary to support expanding enterprise operations while maintaining continuity of Government services. This includes identifying infrastructure constraints, planning capacity improvements, coordinating infrastructure implementation activities, validating operational readiness following infrastructure modifications, and ensuring that enterprise facilities remain secure, reliable, scalable, and capable of supporting evolving operational demands.

The Contractor shall also provide engineering and operational support for the relocation, installation, validation, and decommissioning of enterprise IT infrastructure associated with the movement of ARS personnel, mission functions, and supporting systems to receiving locations throughout the United

States. This includes coordinating physical infrastructure changes, supporting equipment lifecycle activities, validating operational readiness following relocation, and minimizing operational disruption while preserving continuity of Government operations.

All facility infrastructure engineering and operations activities shall be planned and executed to maintain system availability, preserve operational dependencies, protect Government assets, minimize operational risk, and ensure uninterrupted support for mission-critical Government services throughout the BARC transition and phased closure. Work performed under this task shall comply with applicable USDA policies, industry standards, FISMA, NIST SP 800-53, USDA Departmental Manual 3515-001, and other applicable federal cybersecurity and information protection requirements.

2.4 Enterprise Database and Application Operations and Engineering Support

The Contractor shall provide operations and engineering support for the Government's ***Asset Bank Digital Asset Management (DAM) platform*** and the enterprise database environments supporting BARC, BHNRC, USNA, and associated USDA Agricultural Research Service (ARS) Northeast Area (NEA) operations. Asset Bank is a production enterprise application supporting Government asset management and business operations and shall be maintained, secured, and engineered to meet applicable USDA cybersecurity requirements and enterprise security standards while ensuring continuous availability throughout the BARC transition and phased closure.

The Contractor shall provide engineering and operational support necessary to maintain Asset Bank in a secure, reliable, and compliant production environment. Support shall include application administration, configuration management, security hardening, user and role administration, metadata and workflow configuration, vulnerability remediation, security patch management, software upgrades, vendor coordination, database integration, performance monitoring, troubleshooting, operational testing, documentation, implementation of approved enhancements, and technical support necessary to maintain application availability and compliance with USDA cybersecurity and information security requirements.

The Contractor shall support ongoing cybersecurity compliance activities for Asset Bank and associated supporting infrastructure. Activities shall include security control implementation, configuration baseline management, vulnerability assessment remediation, audit support, security documentation updates, coordination with Government cybersecurity personnel and application vendors, implementation of corrective actions, and technical support necessary to maintain compliance with USDA security policies, FISMA, NIST SP 800-53, USDA Departmental Manual 3515-001, and other applicable federal cybersecurity requirements.

The Contractor shall provide operations and engineering support for enterprise database platforms supporting Asset Bank and other Government enterprise applications. Services shall include database administration, configuration management, capacity planning, performance monitoring, security patching, vulnerability remediation, backup and recovery, disaster recovery support, access management, database lifecycle management, data integrity validation, performance optimization, and advanced troubleshooting to ensure secure, resilient, and highly available enterprise services.

The Contractor shall provide engineering support to maintain, enhance, and optimize enterprise applications and supporting databases as mission requirements evolve during the BARC transition and phased closure. Engineering activities shall include application and database integration, architecture assessments, infrastructure coordination, technology refresh planning, performance tuning, operational testing, validation following infrastructure modifications, and implementation of improvements that enhance application reliability, security, scalability, and operational performance.

The Contractor shall also support the preparation, migration, validation, and operational readiness of enterprise applications, databases, and associated data resulting from the relocation of ARS mission functions and supporting systems to receiving locations throughout the United States. Activities shall include identifying application and database dependencies, coordinating technical cutovers, protecting data integrity, validating application functionality following migration, and minimizing disruption to Government operations.

All database and application operations and engineering activities shall be coordinated to maintain system availability, protect Government information, preserve data integrity, minimize operational risk, and ensure uninterrupted support for mission-critical Government services. Work performed under this task shall comply with FISMA, NIST SP 800-53, USDA Departmental Manual 3515-001, USDA cybersecurity policies, and other applicable federal information security requirements.

2.5 Enterprise Storage Infrastructure Operations and Engineering Support

The Contractor shall provide engineering and operations support to maintain, expand, optimize, and transition the USDA Agricultural Research Service (ARS) Northeast Area (NEA) enterprise storage infrastructure as mission requirements evolve during the BARC transition and phased closure. Engineering activities shall support the expansion of storage infrastructure and services at the U.S. National Arboretum (USNA), while planning, migrating, validating, and decommissioning storage infrastructure and associated data supporting mission functions transitioning from the Beltsville Agricultural Research Center (BARC). The enterprise storage environment shall remain secure, reliable, scalable, and continuously available to support mission-critical Government operations throughout the transition.

The Contractor shall provide operations and engineering support necessary to maintain the enterprise storage environment supporting BARC, BHNRC, USNA, and associated enterprise operations. Services shall include storage administration, storage provisioning, capacity planning, storage expansion, performance monitoring, configuration management, lifecycle management, firmware and software maintenance, security patching, vulnerability remediation, backup integration, disaster recovery support, advanced troubleshooting, storage optimization, and technology refresh planning necessary to ensure a resilient and highly available enterprise storage infrastructure.

The Contractor shall continuously evaluate enterprise storage utilization and capacity to support increasing operational demand at USNA and the evolving enterprise infrastructure throughout the ARS Northeast Area (NEA). Engineering activities shall include storage architecture assessments, capacity forecasting, performance analysis, infrastructure optimization, technology recommendations, implementation planning, and validation of storage services following infrastructure expansion, modification, or migration activities.

The Contractor shall provide engineering and operational support for the orderly migration, replication, validation, and decommissioning of enterprise storage resources associated with the relocation of ARS mission functions and supporting systems to receiving locations throughout the United States. Activities shall include maintaining data integrity, coordinating storage migrations, validating successful data transfers, supporting backup and recovery operations, securely sanitizing and decommissioning storage assets when authorized by the Government, and minimizing operational disruption while preserving continuity of Government operations.

All enterprise storage operations and engineering activities shall be coordinated to maintain system availability, protect Government information, preserve data integrity, minimize operational risk, and ensure uninterrupted support for mission-critical Government services. Work performed under this task

shall comply with FISMA, NIST SP 800-53, USDA Departmental Manual 3515-001, USDA cybersecurity policies, and other applicable federal information security requirements.

2.6 Enterprise Infrastructure Monitoring & Patching Management Operations and Engineering Support

As personnel, mission functions, and operational activities continue to relocate to the U.S. National Arboretum (USNA) and other USDA Agricultural Research Service (ARS) locations throughout the United States during the BARC transition and phased closure, the Contractor shall provide enterprise monitoring, patch management, and engineering support necessary to maintain the availability, security, reliability, and operational health of the USDA ARS Northeast Area (NEA) enterprise infrastructure. These services shall ensure continuous operational visibility, cybersecurity, and infrastructure resiliency while supporting the expansion of enterprise services at USNA, the orderly relocation of mission functions, and the decommissioning of infrastructure at BARC.

The Contractor shall provide operations and engineering support for enterprise monitoring and patch management across network, virtualization, compute, storage, database, enterprise applications, Asset Bank, telecommunications, and facility-supporting infrastructure. Services shall include enterprise health monitoring, performance monitoring, alert management, event correlation, configuration management, vulnerability identification, security patch management, firmware and software updates, remediation activities, operational reporting, advanced troubleshooting, and infrastructure optimization necessary to maintain a secure, resilient, and highly available enterprise environment.

The Contractor shall continuously evaluate enterprise infrastructure health, cybersecurity posture, and operational performance to identify risks, optimize system performance, and recommend improvements supporting evolving mission requirements. Engineering activities shall include performance analysis, trend analysis, capacity monitoring, security hardening, configuration baseline validation, implementation of approved technology improvements, and coordination with Government cybersecurity personnel to maintain compliance with USDA cybersecurity policies and enterprise security standards.

The Contractor shall support monitoring and patch management activities associated with infrastructure expansion at USNA, the relocation of enterprise services to receiving USDA locations throughout the United States, and the orderly decommissioning of infrastructure supporting BARC. Activities shall include validating operational readiness following infrastructure modifications, verifying successful implementation of security updates, supporting vulnerability remediation, maintaining operational visibility throughout migration activities, and minimizing disruption to mission-critical Government operations.

All enterprise monitoring, patch management, and engineering activities shall be coordinated to maintain system availability, preserve operational continuity, protect Government information, minimize operational risk, and ensure uninterrupted support for mission-critical Government services. Work performed under this task shall comply with FISMA, NIST SP 800-53, USDA Departmental Manual 3515-001, USDA cybersecurity policies, and other applicable federal information security requirements.

3.0 Period of Performance

September 30, 2026, through September 29, 2027

4.0 Facility Security Requirements

Contractor personnel performing work under this requirement shall comply with all applicable USDA, ARS, facility, cybersecurity, and physical access security policies and procedures while accessing

Government systems, facilities, or operational environments.

Contractor personnel requiring on-site access to Government facilities supporting BARC, BHNRC, and USNA operations shall coordinate access with authorized Government personnel and comply with all applicable escorts, badging, and facility access requirements.

All access to Government systems, facilities, and operational environments shall be limited to authorized personnel and authorized activities necessary to support operational sustainment, cybersecurity activities, continuity of operations, and transition-related support requirements under this contract.

5.0 Primary Area of Contract Performance

Work under this requirement shall be performed primarily at contractor-operated facilities, with on-site support provided at Government facilities supporting BARC, BHNRC, and USNA operations, including locations in Beltsville, Maryland, and Washington, DC.

To support operational sustainment, enterprise infrastructure support activities, and transition-related coordination requirements, contractor personnel shall provide on-site support a minimum of two (2) business days per week, or more frequently as operationally required by Government mission or operational needs.

On-site activities shall be coordinated with authorized Government personnel and performed in accordance with applicable USDA, ARS, cybersecurity, and facility security policies and procedures.

6.0 Government Supplied Resources

The Government will provide the Contractor with access to USDA-ARS NEA systems, facilities, and operational environments as necessary to perform work under this requirement. Access shall be limited to authorized systems, resources, and facilities required to support operational continuity, infrastructure sustainment, cybersecurity activities, and transition-related support functions.

Government-furnished access may include logical access to authorized enterprise infrastructure systems, operational monitoring platforms, facility-related systems, and other interconnected operational environments necessary to support mission-critical operations during the campus transition period.

All Government-furnished resources and access shall be used in accordance with applicable USDA, ARS, cybersecurity, and facility security policies and procedures.

7.0 Minimum Contractor Qualifications & Continuity Requirements

As personnel, mission functions, and operational activities continue to increase at the U.S. National Arboretum (USNA), the Contractor shall demonstrate the technical and engineering capability necessary to expand, secure, and sustain the supporting enterprise infrastructure without disrupting ongoing Government operations. The Contractor shall also demonstrate experience supporting a production enterprise application environment comparable in complexity to the Government's Asset Bank Digital Asset Management platform, including application administration, database integration, security hardening, vulnerability remediation, patch management, vendor coordination, operational testing, and compliance with applicable federal cybersecurity requirements.

Because enterprise systems and data are also being relocated from BARC to receiving USDA locations throughout the United States, the Contractor shall demonstrate experience maintaining uninterrupted production services while planning and executing infrastructure expansion, migration, validation, secure decommissioning, and technology lifecycle activities. The Contractor must possess the operational maturity and technical expertise necessary to engineer and sustain interconnected network, virtualization, storage, database, application, monitoring, cybersecurity, and facility-supporting environments as coordinated enterprise services.

The Contractor's demonstrated experience shall show the ability to maintain system availability, protect Government information, preserve data integrity, support USDA cybersecurity compliance, manage technical dependencies, and minimize operational risk throughout the BARC transition and phased closure. All minimum qualifications identified below are required to establish technical acceptability and must be supported by relevant project descriptions, past-performance information, key-personnel experience, or other verifiable documentation requested by the Government.

a. Enterprise Infrastructure Operational and Engineering Capability
The Contractor shall demonstrate experience providing **Tier II and Tier III enterprise infrastructure operations and engineering support** within an active production environment supporting mission-critical Government or similarly complex enterprise operations. Experience shall include engineering, operations, lifecycle management, technology refresh, capacity planning, performance optimization, and cybersecurity support across interconnected enterprise network, virtualization, storage, database, enterprise application, monitoring, and facility-supporting infrastructure.

The Contractor shall demonstrate experience sustaining production operations while simultaneously supporting enterprise infrastructure expansion, modernization, migration, validation, and decommissioning activities without disrupting operational continuity.

b. Enterprise Network Engineering Capability
The Contractor shall demonstrate experience assuming operational ownership and lifecycle responsibility for an enterprise network environment, including manufacturer warranty administration, Return Material Authorization (RMA) coordination, hardware replacement, inventory and support-entitlement management, configuration backup and restoration, incident response, and restoration of production services following equipment failure. The Contractor shall demonstrate the capability to coordinate directly with Brocade (Ruckus), authorized support providers, and equipment vendors to maintain active support coverage, expedite replacement activities, and minimize network downtime.

The Contractor shall demonstrate experience engineering, operating, maintaining, and expanding an enterprise network supporting multiple locations and interconnected production environments. Experience shall include Brocade (Ruckus) switching infrastructure, configuration management, firmware and software lifecycle management, network monitoring, performance optimization, capacity planning, vulnerability remediation, advanced troubleshooting, and implementation of network modifications.

The Contractor shall also demonstrate experience supporting network expansion associated with increased personnel and operations at USNA and network modifications required for the relocation of mission functions, systems, and enterprise services from BARC to receiving USDA locations. All network activities shall be performed while maintaining availability, security, existing operational dependencies, and continuity of Government operations.

c. Enterprise Virtualization Engineering Capability
The Contractor shall demonstrate experience providing enterprise virtualization operations and engineering support within production environments. Experience shall include virtual infrastructure administration, virtual machine lifecycle management, compute capacity planning, infrastructure optimization, backup integration, disaster recovery support, performance tuning, technology refresh, migration of virtual workloads, and orderly decommissioning of virtual resources.

d. Enterprise Facility Infrastructure Engineering Capability
The Contractor shall demonstrate experience engineering and supporting enterprise IT facility infrastructure, including telecommunications infrastructure, structured cabling, rack and cabinet engineering, power distribution, environmental controls, equipment installation, infrastructure expansion, and technology refresh activities.

The Contractor shall demonstrate experience supporting infrastructure modifications required to accommodate increased operational demand, facility expansion, and relocation of enterprise systems while maintaining continuity of Government or enterprise operations.

e. Enterprise Database and Application Engineering Capability
The Contractor shall demonstrate experience supporting and engineering a production Digital Asset Management (DAM) application environment, including application administration, database integration, security hardening, vulnerability remediation, security patch management, software upgrades, vendor coordination, operational testing, backup and recovery, implementation of approved enhancements, and maintaining compliance with applicable federal cybersecurity requirements. The Contractor shall demonstrate the capability to support a production enterprise application requiring continuous availability, security, and operational continuity.

The Contractor shall demonstrate experience providing operations and engineering support for production enterprise database environments supporting mission-critical enterprise applications. Experience shall include database administration, application and database integration, performance optimization, configuration management, capacity planning, backup and recovery, disaster recovery support, access management, data integrity validation, database lifecycle management, and advanced troubleshooting.

The Contractor shall demonstrate experience engineering and maintaining enterprise applications and supporting databases throughout their lifecycle, including technology refresh, infrastructure integration, application enhancements, migration support, operational validation, and implementation of cybersecurity improvements necessary to maintain secure, resilient, and highly available production environments.

The Contractor shall also demonstrate experience supporting enterprise applications and databases during organizational transition, infrastructure modernization, migration, and decommissioning activities while maintaining uninterrupted production services and protecting Government information.

f. Enterprise Storage Infrastructure and Engineering Capability
The Contractor shall demonstrate experience engineering and operating enterprise storage environments supporting production workloads. Experience shall include storage administration, storage expansion, capacity forecasting, replication, backup and recovery, disaster recovery, performance optimization, secure data sanitization, migration of enterprise data, and orderly decommissioning of storage infrastructure while maintaining data integrity and operational continuity.

g. Enterprise Monitoring, Patch Management, and Cybersecurity Capability
The Contractor shall demonstrate experience providing enterprise infrastructure monitoring, vulnerability management, security patch management, performance monitoring, operational reporting, and continuous monitoring across interconnected enterprise environments.

Experience shall include configuration baseline management, security hardening, vulnerability remediation, incident response support, implementation of security updates, operational health monitoring, and coordination with Government or organizational cybersecurity personnel to maintain compliance with applicable cybersecurity requirements.

The Contractor shall demonstrate the capability to maintain operational visibility across enterprise network, virtualization, storage, databases, enterprise applications, and facility-supporting infrastructure while supporting infrastructure expansion, migration, and technology modernization.

8.0 Information Sensitivity

The Contractor shall adhere to the Privacy Act, Title 5 of the U.S. Code, Section 552a, and applicable agency rules and regulations. The Contractor Program Manager shall ensure that all contract personnel complete required USDA privacy and cybersecurity awareness training.

9.0 Accessibility of Electronic and Information Technology

All information and communication technology (ICT) products and services provided under this requirement shall support operational continuity, maintain compliance with applicable accessibility standards, and align with applicable federal information technology requirements and policies.

This contract vehicle is subject to applicable industry standards. Each information and communication technology (ICT) product or service furnished under this contract shall comply with said standards at a minimum, as specified in the contract. If any furnished product or service is determined to be noncompliant, the Contracting Officer will notify the Contractor in writing. The Contractor shall, without charge to the Government, remediate or replace the noncompliant products or services within a specified timeframe as determined by the Government in writing. If such remediation or replacement is not completed within the time specified, the Government shall have the following remedies:

1) Cancellation of the contract, delivery, task order, purchase, or line item without termination liabilities; or

2) In the case of custom ICT being developed by a contractor for the Government, the Government shall have the right to have any necessary changes made or repairs performed by itself or by another firm for the noncompliant ICT, with the contractor liable for reimbursement to the Government for any expenses incurred thereby.

The contractor must ensure all noncompliant ICT products and services are provided pursuant to

extensive market research and exhibit the highest level of compliance while satisfying the contract requirements.

For every ICT product or service accepted under this contract by the Government that does not comply with industry standards, the contractor shall, at the discretion of the Government, remediate or upgrade the item with a compliant equivalent product or service, if commercially available and cost neutral, on either a contract specified refresh cycle for the product or service, or on a contract effective option/renewal date, whichever shall occur first.

In addition, vendors and contractors shall comply with the standards, policies, and procedures below for all ICT pursuant to this contract:

- For Custom ICT Development Services, the vendor or contractor shall ensure the ICT fully conforms to the applicable industry standards prior to delivery and before final acceptance.
- For Installation, Configuration, and Integration Services, the vendor or contractor shall not install, configure, or integrate the equipment and software in a way that reduces the level of conformance with the applicable industry standards.
- For Maintenance, Upgrades, and Replacements, the vendor or contractor shall ensure maintenance upgrades, substitutions, and replacements do not reduce the original level of conformance with the applicable industry standards at the time of the contract award.
- Service Personnel are ensured by the vendor or contractor to possess the knowledge, skills, and ability necessary to address the applicable industry standards and shall provide supporting documentation upon request.
- When providing Hosting Services, the vendor or contractor shall not reduce the existing level of conformance of the electronic content with the applicable industry standards.
- When purchasing ICT where 1) industry standard validation is not possible prior to award, 2) the ICT will be changed after the award, or 3) ICT will be hosted in a third-party environment, the vendor or contractor shall test and validate the ICT solution for conformance to the industry standards, in accordance with the required testing methods as defined by the agency.
- The vendor or contractor shall document and maintain information regarding the measures taken to ensure compliance with the applicable requirements. This documentation includes but is not limited to testing records, product demonstrations, and reported defects by end users and testers.
- In the case of non-compliance where the vendor or contractor claims its products and/or services satisfy the applicable industry standards specified in the contract vehicle, the contracting officer will promptly inform the vendor or contractor in writing of the non- compliance. The vendor or contractor shall, at no cost to the agency, repair or replace the non-compliant products or services within the period specified by the contracting officer.