United States Department of Agriculture

Farm Production and Conservation

Conservation

<Value Stream Name>

Agile Release Train

Performance Work Statement

PWS Version 0.2

updated: 10/14/2024

Revision History

Date	Version	Description	Author
07/31/2024	0.1	Initial Draft	Kara Cochran
10/1/2024 – 10/14/2024	0.2	Incorporate edits and comments from integrated acquisition planning team	Cavine Phillips Kara Cochran

Table of Contents

1 Background

1.1 Farm Production and Conservation Mission Area

The Farm Production and Conservation (FPAC) mission area is USDA's focal point for the nation's conservationists, farmers, ranchers, producers, forest landowners, as well as federal, state, local, tribal, and private partners, to seek assistance with crop insurance, conservation programs and technical assistance, commodity lending, and disaster programs. FPAC has over 26,000 employees working in 2,200 offices located throughout the fifty (50) States, American Samoa, Mariana Islands, Palau, Puerto Rico, and the Virgin Islands. The FPAC mission area includes four agencies: the Farm Services Agency (FSA), the Natural Resources Conservation Service (NRCS), the Risk Management Agency (RMA), and the FPAC Business Center (FBC).

NRCS provides leadership in a partnership effort to help America's private landowners and managers. NRCS and its predecessor agencies have worked in close partnerships with farmers and ranchers, local and state governments, tribes, and other federal agencies to maintain healthy and productive working landscapes. NRCS works voluntarily with its partners to conserve their soil, water, air, plants, animals, and other natural resources by providing financial and technical assistance based on sound science and suited to a customer's specific needs.

FBC provides mission area-wide administrative functions including information management, financial management, human resources, acquisition management, customer experience guidance, managed services, and more. The Assistant Chief Information Officer for FPAC oversees all FPAC information technology services through the Information Solutions Division (ISD). The Assistant Chief Data Officer for FPAC oversees all FPAC data governance, management, and use.

1.2 NRCS Organization and Vision

NRCS contains seven major lines of business which can be aligned to the NRCS organizational structure of four deputy areas.

Table 1. NRCS Lines of Business.

Line of Business	**Deputy Area (organizational)**
Conservation Planning and Technical Assistance	Programs
Conservation Implementation (Farm Bill Programs)	Programs
Landscape-Level Resources Inventory	Soils Survey and Resource Assessment
Landscape-Level Resources Assessment	Soils Survey and Resource Assessment
Snow Survey and Water Supply Forecasting	Soils Survey and Resource Assessment
Natural Resources Technology Transfer	Science and Technology
Conservation Operations	Management and Strategy

Each Deputy Area has its own unique set of deliverables and products which can focus on internal and external customers including but not limited to farmers and ranchers, local and state governments, tribes, other federal agencies, universities, NGOs and internal NRCS staff.

Within each line of business, NRCS has a variety of programs, at a variety of scales (e.g. field-level or landscape), that it uses to help deliver its mission. Many of the programs provide a specialized technical service, data,

conservation product, and/or conservation practice to help support Farm Bill Programs. Farm Bill Programs are used to provide financial incentives to customers that: (1) help defer the costs associated with implementing one or more conservation practices, (2) help provide incentives to continue with or enhance existing conservation actives, or (3) help purchase conservation easements.

1.2.1 NRCS Programs

1.2.1.1 Background

The Programs Deputy Area includes three divisions. The Financial Assistance Programs Division is responsible for developing policy and implementing financial assistance-focused programs. The Easements Programs Division is responsible for developing policy and implementing easement-focused programs and reporting the count and condition of the Agency's stewardship lands. Conservation Planning and Technical Assistance Division is responsible for developing policy and implementing conservation technical assistance. This involves conservation planning and all the technical field-level assistance including implementation of conservation programs and practices at the field-level. Conservation planning involves a nine-step process which mirrors a basic problem-solving approach. The primary customers for these divisions are farmers and ranchers. NRCS State, Area, and Field-level staff implement the various programs supported by these divisions.

1.2.1.2 Vision

Language from the 2018 Farm Bill charged NRCS to continue streamlining and integrating its Farm Bill Programs business processes. Thus, NRCS currently is transitioning processes, policies and supporting software applications to meet these expectations. In March 2020, NRCS deprecated its legacy conservation planning software (Customer Service Toolkit) and replaced it with Conservation Desktop (CD). CD is an integrated system that allows users to seamlessly access a customer's technical and financial assistance data including geospatial, tabular, electronic documents/content, and electronic signatures.

In 2018, NRCS also initiated the idea of program neutral resource assessments and ranking. To help facilitate these processes, NRCS developed and deployed the Conservation Assessment Ranking Tool (CART) in January 2020. CART was designed to collect inventory data and assess a potential conservation plan based on the resource assessment results. CART determines the assessment's Farm Bill Program eligibility. At that time, a client would select the financial assistance program(s) they may want to apply for and a scoring and ranking of that assessment is conducted in CART. A system named ProTracts currently handles most of the application and financial assistance contracting part of the business process.

NRCS plans to continue its integration efforts between CD and CART along with migrating the application and contract management functionality from ProTracts to CD. This will include additional enhancements to CD and CART to incorporate the automation of its environmental evaluation process which is required when creating conservation plans. NRCS will leverage the data being collected in CART and CD to begin reporting conservation outcomes and effects. NRCS plans to incorporate its easements data from the current National Easements Staging Tool (NEST) into CD and implement additional functionality needed to support easement acquisition and monitoring. Another part of the future vision for NRCS is to leverage mobile data collection that integrates with CD. Additionally, NRCS plans to continue CD's integration with its customer-facing web portal Farmers.gov. In the future, clients will be able to submit online requests for conservation assistance, submit electronic documents, electronically sign documents, and receive notifications from various applications that are part of CD.

NRCS also is accelerating into its long-term vision for geospatial conservation data. Conservation Geo is ramping up to support NRCS data quality, data governance, and data delivery processes and support the states and leadership with authoritative data. The partnership between Conservation Geo and the Dynamic Soils Hub provides a solid foundation and pathway for NRCS to achieve its long-term goals for high-quality decision support for conservation and compliance with the Geospatial Data Act of 2018.

1.2.2 NRCS Soil Science and Resource Assessment

1.2.2.1 Background

Soil Science and Resource Assessment (SSRA) helps answer the important questions that strengthen NRCS's voluntary conservation delivery by collecting and analyzing data and developing tools critical to conservation planning. While conservationists work with agricultural producers and conservation partners to draft conservation plans and implement conservation practices, SSRA staff works with members of academia, researchers, and other science partners to provide mission-critical data, findings, and other information to support science-based, data-driven conservation. Across customer groups and geographic scales, NRCS' SSRA Deputy Area — including the Soil and Plant Science Division (SPSD), National Water and Climate Center (NWCC), and Resource Inventory and Assessment Division (RIAD) — plays an integral role in NRCS's approach to conservation. SSRA has more than 600 staff nationwide.

Within the SSRA Deputy Area there are two divisions: Resource Inventory and Assessment Division and Soils and Plant Science Division. The SSRA Deputy Area also has operational control over the National Water and Climate Center (NWCC). The Resource Inventory and Assessment Division is responsible for conducting the National Resources Inventory which as a program collects and produces scientifically credible information on the status, condition, and trends of land, soil, water, and related resources on the Nation's non-federal lands. The division is also responsible for conducting assessments and modeling of conservation efforts to determine outcomes and effects of NRCS' conservation activities.

The Soils and Plant Science Division is responsible for the inventory and analysis of soil and plant resources throughout the United States. They map soils and provide geospatial soils information along with detailed information about the physical and chemical properties of soils. The Division is also responsible for the collection of plant related data. The NWCC is responsible for providing data collection and water supply forecasts for a variety of purposes (e.g. hydroelectric dam operations, reservoir management and drought assessment). The National Plant Data Team, physically located at the East National Technology Center (ENTC), provides national and international leadership on plant information for the United States. The Team acquires, develops, and disseminates plant information to support USDA, NRCS, and other efforts to improve the ecological health of the land. The Team maintains the PLANTS Database to support a variety of conservation activities.

The SSRA Deputy Area works closely with FPAC-BC ISD Geospatial Enterprise Operations (GEO) as there is a geospatial component with almost every SSRA Deputy Area IT product. ISD GEO is responsible for technical leadership and expertise in geosciences: mapping science, cartography, geographic information systems (GIS), aerial photography, remote sensing, and global position systems (GPS), elevation and imagery data, natural resources data, and geospatial technology. The various divisions within the SSRA Deputy Area service a vast customer base including individual farmers and ranchers, NRCS staff, universities, industry, federal, state, and local agencies, non-governmental organizations, congress, tribes, and the non-farming community.

1.2.2.2 Vision

Going into the future, the SSRA Deputy Area intends to modernize and maximize automation for soil, plants, and ecological sites resource inventory supporting tools to enhance the customer services through adaptable, efficient, scalable technical solutions to streamline processes to free up resources for mission critical work. It also intends to eliminate the risks associated with outdated technology to increase efficiency, data integrity, quality, and availability. Integrating and automating data with other business processes, especially the conservation delivery process is a major priority as well.

The Dynamic Soils Hub (DS Hub) under the Natural Resources Conservation Service (NRCS) is an innovative platform designed for authoritative soil geospatial modeling. It aims to provide tools and data for both internal and external partners and stakeholders, enabling high-performance geospatial modeling and terrain analysis.

The DS Hub connects soil and conservation databases, allowing for the assessment of environmental benefits in conservation programs by accessing previously siloed data and models across Agency divisions. This expands the USDA's capacity to model and report on soil properties that change with conservation management over time. Key features of the DS Hub include:

- Access to both external and internal authoritative data sources and soils data for robust soil modeling.
- An innovative geospatial data user interface specializing in unique terrain analysis, enabling users to create new data products from a variety of existing authoritative datasets.
- No-code processing of large data volumes for geospatial modeling, unlike current tools and workflows.
- Collaboration tools for modelers to work on projects, share data and experiments, and produce scientific models and datasets.
- Enhanced USDA capacity to model and report on soil properties that change with conservation management.
- Facilitation of the collection, storage, and delivery of data related to dynamic soil properties and conservation management.
- A focus on rapidly responding to customer requests for science-based soil property data at the Deputy Chief, Chief, and Undersecretary levels.

The Soil Business Systems Branch intends to modernize and integrate their information systems to meet customers' needs, mission requirements, and to support putting conservation on the ground. Within the same timeframe, the Branch intends to adapt new technologies and applications to address emerging trends in soil and plant sciences. The Ecological Sites Branch intends to have the Ecosystems Dynamic Interpretative Tool (EDIT) program within the family of the soil and plants information systems, integrating it with other conservation programs support tools.

The National Plant Data Team plans to modernize its PLANTS database and website to include a dynamic content manager as well, as increasing the processing and delivery of information to our customers. The team is planning to upload the multi-year backlog of plants data and develop and implement product delivery metrics.

The Soil Survey Research and Laboratory intends to improve the management of laboratory data systems and leverage improvements of the soil and plants data systems to use the combined information in streamlined inventory delivery.

The Soil Surveys Standards Team intends to evolve training methods to support new technologies, products, and processes in support of natural resources inventory and conservation. They are also planning to develop and maintain scientific world-wide natural resources inventory standards to support conservation that is fact-based, data-driven, science-based, and customer focused.

In addition, the Snow Survey and Water Supply Forecasting Program intends to increase the time spent on interpretation of collected, aggregated, and ingested telemetry data and decrease the time spent on work-around processes, as well as a reduction in the reliance on outdated and aging enabling technology so that the program provides better decision-support products to our conservationists, farmers, ranchers, producers, as well as federal, state, local, tribal, and private partners. They also plan to eliminate the risks associated with aging and outdated technology to increase efficiency, data integrity, quality, and availability along with modernizing the technologies needed to improve forecasting and business analysis process, accuracy, reliability, and availability.

The Resource Inventory and Assessment Division (RIAD) is planning to integrate some of the currently external applications with existing NRCS databases and systems. For example, updates and integrations are planned for the Rangeland Brush Estimation Toolbox (RaBET) so they can complete data updates to all 39 NRCS Major Land

Resources over the next five years. RIAD will continue to utilize the Rangeland Analysis Platform (RAP) to help improve Conservation Effects Assessment Project (CEAP) modeling efforts by adding additional geospatial layers. RIAD is planning for enhancements to the Soil and Water Resource Conservation Act (RCA) web-based dashboard and appraisal reports solution used to provide broad natural resource strategic assessments to Congress.

The FPAC GEO supports the SSRA deputy area in several ways. GEO's future efforts focus on the modernization of the Geospatial Data Gateway (GDG) while continuing to maintain the current version. which is the One Stop Source for environmental and natural resource data, at any time, from anywhere, to anyone. This service is made available through a close partnership between the three USDA Service Center Agencies (SCA): NRCS, FSA, and Rural Development (RD). Planning is underway for the cloud-based, FEDRAMP certified replacement of this legacy solution.

GEO has begun migration to Amazon Web Services (AWS) where they will continue to provide support for the data and resources of the authoritative data marts including the Resource Data Gateway (or its replacement), Geospatial Services, High Resolution Elevation Data Mart, and Remote Sensing Data Mart. The current migration to AWS will continue to provide for the information lifecycle management of geospatial data used in NRCS agency programs, as well as programs within FSA and RD.

GEO also plans to focus on the High-Resolution Elevation Data Mart which provides visualization and analysis for high resolution elevation data along with the provisioning of derivative elevation products and services for use in conservation planning and design, environmental assessment, and terrain mapping activities. Finally, GEO also needs to continue maintaining and improving the Remote Sensing Data Mart (RSDM) and Remote Sensing Lab File Management System, a web portal and file management system for accessing remote sensing data. The RSDM's and RSLFMS's primary functions are to support the geospatial needs of the National Resources Inventory program. It also provides for the access of remotely sensed imagery and data supporting other program areas such as the Wetland Reserve Program.

1.2.3 NRCS Science and Technology

1.2.3.1 Background

Within the Science and Technology (S&T) Deputy Area there are three divisions: Conservation Engineering Division, Ecological Sciences Division, and Soil Health Division. The S&T Deputy Area also maintains operational control over five centers including: National Water Management Center, East National Technology Support Center (ENTSC), Central National Technology Support Center (CNTSC), the West National Technology Support Center (WNTSC), and National Design, Construction and Soil Mechanics Center.

The Conservation Engineering Division is responsible for creating, maintaining, and disseminating all engineering-related policy, technical design standards, and engineering specifications for NRCS conservation practices. The Ecological Sciences Division is responsible for providing and disseminating technical expertise and information related to grazing, biology, wildlife, water quality, nutrient management, invasive plant species, conservation compliance, forestry, agronomy, rangeland, air quality, and energy. They also are responsible for the technical design specifications for NRCS non-engineering related conservation practices. The Soil Health Division is responsible for maintaining technical expertise, providing support, and disseminating technical information regarding soil health (i.e. the capacity of the soil to function as a living ecosystem).

The National Water Management Center is responsible for the application of hydrology and hydraulics to all NRCS programs. It provides direct assistance, the latest technology transfer and delivery, direct technical assistance, water resources planning, watershed policy implementation, and program support with an emphasis on consultation and training of State personnel. The National Design, Construction and Soil Mechanics Center provides technical support for design, construction, operation, and rehabilitation of complex engineering projects essential to resource conservation, environmental enhancement, and agricultural productivity.

The ENTSC is responsible providing direct conservation technology transfer to NRCS state and field staff for the eastern portion of the United States. The center is also home to two national teams: National Animal Manure and Nutrient Management Team and National Plants Data Team. The National Animal Manure and Nutrient Management Team provides livestock, manure management, and nutrient management research findings, project updates, and information to staff and partners. It also evaluates new technology for manure handling, nutrient management, land application, and alternative manure use. The Team integrates current research and development into tools and practices for delivering assistance to livestock and other producers.

The CNTSC is responsible for providing direct conservation technology transfer to NRCS state and field staff for the central portion of the United States. The center is also home to the National Grazing Lands Team responsible for providing national technical leadership for ecologically based technology development in all areas of grazing lands management and conservation. In addition, the center is nationally responsible for providing technical leadership for wetlands and wildlife.

The WNTSC is responsible for providing direct conservation technology transfer to NRCS state and field staff for the western portion of the United States. The center is home to the National Energy Team, National Air Quality and Atmospheric Change Team and the National Water Quality and Quantity Team. The Energy Team develops and delivers information and technology that addresses energy conservation in agricultural systems and natural resource issues related to the production, utilization, and management of renewable energy sources such as biofuels, solar, and wind. The Air Quality and Atmospheric Change Technology Development Team works with NRCS specialists and policymakers, as well as other Federal, State, University, and private organizations to provide agricultural air quality technology and information to NRCS personnel, NRCS partners, and the public. The Water Quality and Quantity Team develops and delivers cutting edge tools and training to address natural resource concerns related to hydrology and hydraulics, nutrient management, pest management, soil erosion, irrigation water management, agricultural drainage, salinity, and stream restoration.

1.2.3.2 Vision

Currently, the S&T Deputy Area maintains over 110 different software applications to perform various technical assessments, designs, and provide technical information. Many of these applications were developed many years ago and may reflect older technical techniques and assessment calculations. Moving into the future, efforts will be made to modernize, enhance, and (in some cases) integrate these applications with one another or conservation planning systems.

The S&T Deputy Area is seeking to develop and maintain technical excellence within the agency to acquire, deliver, develop, and identify science and technology to provide world-class technical assistance to both internal and external customers. To accomplish this, NRCS will: (1) maintain science-based practice standards; (2) identify, analyze, and integrate new science and technology into practice standards; (3) develop and maintain resource concerns; (4) provide current up-to-date technology, tools, and technology transfer methods; and (5) reduce dependency on operating systems.

NRCS plans to improve conservation technical assistance process efficiency while emphasizing quality outcomes through analysis of enterprise relationships, process and technology interdependencies, practice utilization, and existing as well as emerging automation enablers. To achieve this NRCS is planning to integrate Job Approval Authority and certified conservation planner status into Conservation Desktop and manage payment schedule information.

Going into the future, NRCS wants to maintain an understanding of and connection with S&T and USDA customers, both internal and external, and identify their needs to ensure proper alignment of services, service delivery methods, and technology to achieve agency goals. To accomplish this, NRCS will: (1) integrate science-based and economic information into programmatic payment schedules; (2) complete resource inventory and

assessment for each resource concern, as they are relevant to the customer; and (3) generate implementation requirements for all conservation practices scheduled in conservation plans.

NRCS also is planning to become information rich through the collection and delivery of science and data from authoritative sources, observation of the land, analysis of resource data, and dissemination of information through multiple channels. To accomplish this, NRCS plans to: (1) provision geospatial datasets that identify areas with significant resource concern occurrence by characterization of terrain, hydrology and vegetation phenomena derived from high resolution elevation and imagery derivatives; (2) provide pre-built geospatial information to locate opportunities for conservation practice application that are based on analysis of terrain, hydrology, soils, and land use history; and (3) be able to conduct automated and manual analysis for resource inventory, assessment, and implementation requirements in both office and on-site work environments.

As part of its future vision, S&T Deputy Area wants to assess and manage natural resource information and natural resource technology to meet strategic objectives, agency accountability requirements, and program requirements while minimizing agency costs. Achieving these goals will require NRCS to: (1) keep information on dams and watershed projects; (2) maintain technical information associated with conservation activities and Technical Service Provider requirements with transparency to the public; and (3) provide transparency to the public and internal access to all technical references, resources, and data used by NRCS field employees for conservation planning efforts.

Part of NRCS' congressional mandates include maintaining a national inventory of NRCS-assisted dams as well as additional NRCS watershed program data. The database contains approximately 29,000 dams. NRCS is also required to maintain and submit to the Army Corp of Engineers (on a bi-annual basis) dams inventory data for all dams meeting the inventory requirements. To accomplish this, NRCS will continue to maintain and (when necessary) enhance its dam inventory application.

Moving into the future, NRCS needs to effectively track highly erodible land and wetland compliance (HELC/WC) determination requests from start to finish, including automated integrated workflows with its sister agency, FSA. This will require NRCS to have the ability to: (1) consistently record wetland determination boundaries in a national geodatabase; (2) consistently record past wetland determinations in a geodatabase with a link to stored documents to prevent duplication of work; (3) make HELC/WC information readily viewable to NRCS in client interface; and (4) record results of HELC/WC compliance field reviews.

NRCS' future vision also includes integrated geospatial data resources that inform National Environmental Protection Act (NEPA), National Historic Protection Act (NHPA), and Endangered Species Act (ESA) compliance on conservation activities and providing conservation practices that would otherwise be acquired through state level agreements, nationally into NRCS conservation planning software. To complete this, NRCS plans to: (1) enable flexibility for state modifications to meet different state agency requirements and data availability; (2) develop base geospatial data to help automate environmental evaluation activities; (3) develop a national-level agreement with all state historical preservation offices (SHPOs) to assist with more standardized and timely access to SHPO data/consultation; and (4) develop a national agreement with US Fish and Wildlife Service to improve access to their authoritative ESA datasets and web services.

Finally, the S&T Deputy Area also wants to provide transparency to the public on findings from innovative projects and new technologies (e.g. Conservation Innovation Grants (CIG) on-farm trials, soil health demos and Regional Conservation Partnership Program (RCPP)). To do this, NRCS needs a back-end management and customer-facing portal for searching and data entry. The portal would provide links to references and data stores that NRCS currently maintains on resource information, effects of conservation activities, and practice implementation data.

1.2.4 NRCS Management and Strategy

1.2.4.1 Background

The Management and Strategy Deputy Area (M&S) plays a key role of support to the NRCS workforce by ensuring the NRCS workforce can perform both operationally and technically. The M&S Deputy Area contains seven divisions: Appropriations & Allocations Division, Business Resources Management Division, International Programs Division, Operations Support Division, Outreach & Partnerships Division, Policy & Accountability Division, and Technical Training & Development Division.

The **Appropriations & Allocations Division** manages the agency budget in coordination with the FPAC Business Center.

The **Business Resource Management Division** provides mission support services through human capital planning & management, strategic planning, data analytics, project management, and process analysis. The Division will also serve as a coordinating function within the Management and Strategy Deputy Area functions as well as across Deputy Areas in NRCS.

The **International Programs Division** provides mission critical coordination of global conservation and technical assistance.

The **Operations Division** provides advisement and management of operational support services, including logistical and infrastructure support.

The **Outreach and Partnerships Division** works within NRCS to provide mission critical guidance and support to staff at all levels supporting outreach and partnership activities. The division provides consistent outreach guidance for the agency through support to state outreach, partnerships staff, and management of cooperative agreements.

The **Policy and Accountability Division** provides oversight for the development of agency policy across all deputy areas and states. This includes providing highly complex analysis to ensure the agency policy remains current and in alignment with statute and regulation.

The **Technical Training and Development Division** provides mission critical developmental needs to the agency's workforce. The division is responsible for providing comprehensive, specialized, and timely training programs that enhance the technical competence of the NRCS workforce that leads to improved service delivery.

1.2.4.2 Vision

Going into the future, the M&S Deputy Area intends to focus on the implementation of a new Mission Support Project Management system that would improve process management by implementing functionality that: (1) processes intake requests, (2) automates common workflows and tasks, (3) stores and manages documents, (4) monitors deadlines, (5) provides reporting capabilities, and (6) interfaces with existing tools. The system will leverage the latest project management technologies available to enable staff to focus on analysis, integration, process improvement, collaboration, and other complex tasks.

Additional NRCS business processes this technology could improve includes funds verification, data call administration, decision tracking, operating budgets, records management, public-facing webpages such as eDirectives, and quality control. Future functionality could also impact initiative requests and approvals, tracking initiative outcomes, contracts, conferences, meetings, travel, working capital funds, suspension, and debarment, tracking for certification of budget reporting, training, and human resources.

M&S is also focused on the National Office Information System (NOIS). The goal of NOIS is the development and implementation of a comprehensive, enterprise-wide authoritative national office information system, linked to

other FPAC mission area-wide authoritative sources of operational and programmatic data, to facilitate the more effective and efficient mission support, thereby optimizing service to our internal and external customers.

M&S will provide comprehensive, specialized, and timely training programs/tools that enhance the technical competence of the NRCS workforce that leads to improved service delivery. Career Planner will be one of these tools. A career planner is an interactive training plan that details the tasks that an employee needs to accomplish to do their job successfully. It is designed to help employees identify what training is needed in their current grade level and as they continue with their career at NRCS. NRCS will use the career planner for training and development purposes to add consistency and structure to training across the organization. Because career planners set standard expectations, they are an excellent starting point for painting a picture of the expected knowledge, skills, and abilities of the workforce. This provides employees with target competencies and behaviors across the range of proficiency levels for training and developmental experiences.

Finally, NRCS needs to update critical mission delivery systems to support digital records management along with making select document management UI/UX enhancements. To support the document management effort, there is integration work that is needed to support many NRCS applications including but not limited to the following systems: Programs Portal, DamWatch, Field Office Tech Guide (FOTG), Conservation Practice Documents – Document Management System (CPD-DMS), National Easement Staging Tool (NEST), National Engineering Tool Suite (NETS), WinPond, Conservation Desktop – Document Management System (CD-DMS), ProTracts, Guardian and Farmers.gov.

1.2.5 Value Streams

NRCS has a variety of programs, products, and customers. NRCS programs' functionality, databases, and systems align to NRCS Value Streams. Each value stream represents the series of steps used to implement work and provide a continuous flow of value to NRCS. An NRCS information technology capital investment may contain one or more value streams. The current NRCS Value Streams are:

1. Core Natural Resource Information Systems – Functionality to support the integration of science models and development of resource databases; and systems that collect, analyze, and deliver data and information that contribute to the success of all internal agency and public natural resources programs. This generally aligns with the Soil Science and Resource Assessment Deputy Area.
2. Water and Climate Information Systems - Functionality, databases, and systems needed to provide water, snow, and climate monitoring data, collection and predictions, forecasts, and products. This generally aligns with the Soil Science and Resource Assessment Deputy Area.
3. Conservation Practice Implementation - Tools and systems needed for developing Component Plans (e.g., Nutrient Management Plan, Forest Management Plan, etc.), and Conservation Practice Implementation Requirements, Designs, and Checkout. This generally aligns with the Science and Technology Deputy Area.
4. Conservation Plan and Compliance Information - Functionality, databases and systems needed to work with clients to develop a basic conservation plan. Including steps 1-7 of the conservation planning process. This aligns with the Programs Deputy Area.
5. Conservation Programs Contracts and Agreements – Functionality and systems needed to rank applications, develop, and manage landowner agreements/contracts and partnership agreements used to implement conservation programs. This aligns with the Programs Deputy Area.
6. Operational Management & Supporting Systems - Functionality and databases that track and report agency operational management, as well as the status of progress and accomplishments toward delivering the NRCS mission, both internal and external facing. This aligns with the Management and Strategy Deputy Area.

7. Natural Resource Document Management Systems – Functionality and systems that manage the storage, searching, routing, records management and the digital use of critical agency documents and information internally and externally. This aligns with the Management and Strategy Deputy Area.

1.3 FPAC Information Solutions Division

The FPAC Information Solutions Division (ISD) is led by the FPAC Assistant Chief Information Officer and has six branches: Information Assurance, Service Strategy and Planning, Customer Needs Management, Business Operations, Service Delivery and Operations, and Geospatial Enterprise Operations.

The Service Strategy and Planning Branch conducts IT strategic planning in alignment with Departmental direction, formulates IT policies and procedures in support of Department and industry standards, and provides strategic and tactical architectural and design guidance throughout the Systems Development Life Cycle (SDLC). The Information Assurance Branch manages an information assurance awareness program, access controls, and information assurance incidents and events. The branch is also responsible for implementing an IT Privacy Program, in consultation with the Department and Agency Privacy Officer.

The Customer Needs Management Branch establishes, manages, and maintains strategic relationships with FPAC stakeholders and customers to define FPAC business roadmaps and requirements. The branch also defines IT project management methodologies, policies, and procedures; and provides project managers across ISD for software and solution delivery projects. The Business Operations Branch manages execution of the FPAC IT capital investment budget and oversees FPAC IT contracts and agreements in adherence with Departmental and OMB policy and guidance.

The Service Delivery and Operations Branch (SDOB) develops, configures, tests, implements and maintains high-quality IT services and solutions to fulfill FPAC mission requirements. SDOB provides leadership and direction in the administration of ISD operational infrastructure environments, databases, tools, and services including data warehousing and business intelligence environments. Additionally, the branch serves as the primary point of contact with USDA service providers, such as the USDA Client Experience Center (CEC) and USDA Digital Infrastructure Services Center (DISC) to manage FPAC infrastructure and end user computing needs. Within SDOB, the Conservation Section delivers IT services and solutions supporting the NRCS lines of business.

The Geospatial Enterprise Operations (GEO) Branch [enter information about the GEO organization/operating model here]

1.4 FPAC Office of the Assistant Chief Data Officer

FPAC established a centralized analytics team, Office of the Assistant Chief Data Officer, (ACDO) which helped establish a framework for long-term adoption and management of analytics across the mission area. The establishment of ACDO has assessed organizational structures as well as the data infrastructure to provide insight into how FPAC can better position itself for long-term, sustained success in the areas of data & analytics. ACDO oversees establishing mature data governance processes and stewardship.

The ACDO team identifies and helps solve major cross-cutting strategic questions by bringing the use of data analysis and advance data analytics techniques and methods to bare. This includes machine learning and artificial intelligence. The ACDO team also provides oversight on the creation of analytics products such as data visualization, scenario analysis tools, and prescriptive/predictive models to draw insight from Mission Areas' vast data- structured, semi-structured data and unstructured, for day-to-day use by business leaders. NRCS and Conservation Branch will be supported by the ACDO team to cultivate a data-driven organization through the development and enablement of their workforce (fostering and championing data science training and sourcing

talent in support of and/or NRCS). The team will work with NRCS to formulate and align overall Mission Area data strategy and data governance in partnership with NRCS leadership and Information Solutions Division. Ensuring data is easily accessible yet secure, is of high quality and can be transformed into new formats and knowledge.

ACDO team will oversee the planning, review and implementation of data/analytics platforms and tools across the mission area to improve links between siloed databases and data stores that NRCS needs to support their business operations. They will coordinate with the USDA Chief Data Officer on NRCS and other FPAC Agencies behalf to enable open data, participate in inter-Departmental activities and ensure that relevant data is readily available, easily found and easily reusable across the Department.

ACDO team will closely work with the department on help achieving department wide data goals and help develop planning the roadmap and strategies. ACDO team will develop Data and AI strategies for mission area and partner with agencies on the implementation of the tactical outcome of those strategies.

1.5 Conservation Information Technology Services

USDA recognizes that conservation by farmers, ranchers and forest owners today means thriving and sustainable agriculture for our future. Seventy percent of the nation's land is privately owned, and conservation of our nation's private lands not only results in healthy soil, water, air, plants, animals, and ecosystems, it also provides productive and sustainable working lands.

The ISD Conservation Section, ISD GEO branch, and Office of the ACDO work to provide IT and geospatial services supporting NRCS lines of business. IT service delivery is supported by multiple federal contracts for IT services and products including Software-as-a-Service (SaaS), commercial-off-the-shelf (COTS) solutions, software application development and maintenance, production application hosting support, security services, quality assurance testing, and helpdesk services. Federal employees and contractors work collaboratively across organizational and contract boundaries to deliver integrated services seamlessly and effectively. NRCS program success relies on a delivery-focused approach to providing IT services.

1.5.1 Business Capability and IT Modernization Roadmaps

NRCS maintains a Business Capability Roadmap a to define, prioritize, and approve work supporting NRCS IT service delivery by value stream. Work is defined by epic, a collection of related features. The Business Capability Roadmap establishes priorities by value stream for a rolling three-year period and may include set delivery dates for some epics based on NRCS program delivery needs. The current NRCS Business Capability Roadmap (attachment X) is included in the performance work statement for reference and to help the contractor understand the current NRCS business vision.

ISD maintains a three-year IT Modernization Roadmap which aligns to the USDA Modernization Roadmap. The IT Modernization Roadmap guides IT delivery approaches and influences the NRCS Business Capability Roadmap priorities. Some IT modernization goals work towards set delivery dates based on USDA-wide targets. Other IT modernization goals foster a continual focus on modern IT delivery.

The roadmaps are maintained dynamically, reviewed and re-prioritized quarterly, and work is authorized by the NRCS Investment Review Board annually. The NRCS Investment Review Board may authorize additional work during the year based on emerging or evolving business priorities or IT modernization impacts. All work authorized under a roadmap drives toward achievement of the value stream future state defined in the performance work statement.

1.5.2 Integrated Components

Delivery of IT services supporting NRCS lines of business requires cohesive integration of multiple federal and contractor teams. USDA uses Scaled Agile Framework (SAFe) to provide a framework for integration and execution of Agile software delivery services.

1.5.2.1 Solution Agile Release Train

The Solution Agile Release Train (ART) adds value to NRCS by facilitating and improving the overall Conservation Solution strategy to ensure alignment with NRCS and Business requirements. Roles and responsibilities of the Solution ART include but are not limited to:

- Cross-ART coordination, communication, support and program increment (PI) planning
- Creation, refinement, and prioritization of Solution-level and approved portfolio-level backlogs
- Management of solution-level risks, dependencies, and impediments
- Cross team and train collaboration and coordination/facilitation
- Continuous process improvement, support, and training
- Maintenance, management, and technical oversight of Solution-level architecture and technical solutions
- Status reporting

1.5.2.2 Value Stream ARTs

NRCS Value Streams are delivered by ARTs. Each ART maintains a portfolio dedicated to building and supporting a set of solutions, which are the products, services, or systems (applications) delivered to NRCS. The five active Value Stream ARTs are:

- Odin ART – supports the Core Natural Resource Information Systems and Water and Climate Information Systems value streams
- Prometheus ART – supports the Conservation Practice Implementation value stream
- Metis ART – supports the Conservation Plan and Compliance Information value stream
- Money ART – supports the Conservation Programs Contracts and Agreements value stream
- Olympia ART – support the Operational Management and Supporting Systems and the Natural Resource Document Management Systems value streams.

1.5.2.3 IT Operations – Platform Team

1.5.2.4 System Engineering and Technical Assistance (SETA) ART (ART)

The System Engineering and Technical Assistance (SETA) team compiles data and metrics, performs analysis, and provides recommendations to the Government to improve software quality, mature Scaled Agile Framework (SAFe) processes, and improve delivery of systems, applications, and software. The team ensures software products, regardless of the contract vehicle or vendor delivering artifacts, support the single vision of NRCS end state and present a unified product to the end-user.

1.5.2.5 Value Management Office ART (VMO ART)

The Value Management Office (VMO) primarily supports the strategic program and portfolio management of all Conservation efforts under the Conservation Section Branch Chief. The VMO coordinates value streams in relation to products and funding, supports program governance and execution, and fosters data and operational excellence. These efforts are layered into various categories of support including:

- *Portfolio Management Support,*
- *Branch Chief & GPM Project, Program, and Tactical Level support,*
- *SDLC & Governance Support,*
- *Section Related Data Management, License Management and Knowledge Management.*

1.5.2.6 Other Program Integration Points

1.5.3 Key Stakeholders

NRCS IT service delivery involves a multi-functional team of stakeholders working in tandem. Key stakeholders and their roles are defined here. This is not an exhaustive list of stakeholders involved in IT service delivery.

1.5.3.1 Government Product Owner

The NRCS Government Product Owner (GPO) is the Federal Government's business representative that is primarily responsible for maximizing and documenting the delivery of business value delivered by the team by ensuring that the team feature backlog is aligned with customer and stakeholder needs. As a member of the extended Product Management function, the GPO is the team's primary customer advocate and primary link to business and technology strategy. The GPO oversees the backlog and acceptance criteria at the feature level. The GPO coordinates with the Government Business Owner (GBO) to ensure that product activities align with the overall business and technology strategy. This coordination and governance are documented in the Government's designated requirements management tool.

1.5.3.2 Government Business Owner

The NRCS Government Business Owner (GBO) is the Federal Government's business representative for all applications that align to the ART (ART) value streams defined within the contract scope. The GBO coordinates with the GPOs to ensure ART prioritization is clearly defined and meets the customer and stakeholder needs. The GBO oversees the portfolio backlog and acceptance criteria at the portfolio epics and program epic level and works with the Mission Delivery Optimization (MDO) team to ensure the ART deliverables at the portfolio epic level are aligned to the approved Business Capability Roadmap. The GBO also coordinates with the Government Program Manager (GPM) to provide strategic direction, remove blockers, and provide feedback on vendor performance throughout the contract.

1.5.3.3 Government Program Manager

The Government Program Manager (GPM) is the Federal Government's Information Solutions Division (ISD) representative for all applications that align to the ART (ART) value streams defined within the contract scope. On behalf of the ISD Conservation Section Chief, the GPM monitors the execution of the contract that governs this performance work statement. The GPM coordinates with vendor leadership to ensure that work efforts are executed in accordance with contract guidance and USDA/NRCS, and industry best practices, as well as ensures

that project schedule and scope remain in line. Additionally, the GPM coordinates with all stakeholders on problem resolution at the Federal level, when these problems cannot be resolved by the vendor.

1.5.3.4 Tactical Project Manager

The NRCS Tactical Project Manager (TPM) assists the GPM in monitoring the execution of the of the contract that governs this performance work statement. The GPM can delegate tasks, as needed, to ensure that contract deliverables are on time. TPMs *are not authorized* to perform any GPM tasks that include user access or authorization requests, changes to the PWS, or project budget.

1.5.3.5 NRCS Mission Delivery Optimization (MDO) Team

The NRCS MDO team manages the strategic NRCS Business Capability Roadmap (also referred to as the IT Roadmap), Value Stream product designations and overall training and dissemination of information technology details to all Government Business Owners and Government Product Owners. MDO will also help identify cross train dependencies and guide coordination to ensure that all ARTs are creating products that have the same look, feel, and functions as they appear to the end user. MDO also coordinates user acceptance testing (UAT), training, and user guides. MDO works across all NRCS Deputy Areas to manage the NRCS portfolio and the business priorities.

1.5.4 Definitions

(Government is documenting these definitions.)

Defect

Acceptance Criteria

Acceptance Criteria are specific to individual backlog items (features, stories), detailing the conditions that must be met for the requirement to be considered complete. These are typically defined by the user/

Feature Readiness (Definition of Done)

Definition of done is a broad checklist that applies to every single Product Backlog Item (features, stories), ensuring consistency and completeness. These are typically defined by the development team.

Enabler

Enablers are backlog items that extend the architectural runway of the solution under development or improve the performance of the development value stream. Enablers are captured in backlogs as a type of Feature, or Story.

Enablers are used primarily for exploration, architecture implementation, refactoring, building infrastructure, and addressing compliance. While their type is unique, they are managed similarly to customer-facing backlog items.

Feature

A Feature represents solution functionality that delivers business value, fulfills a stakeholder need, and is sized to be delivered by an ART within a PI.

Each feature includes a benefit hypothesis and acceptance criteria and is sized or split as necessary to be delivered by a single ART in a PI.

Objectives

Objectives summarize the business and technical goals that teams and trains intend to achieve in the upcoming PI and are either committed or uncommitted. The team should not include more than 2-3 uncommitted objectives, per PI.

Committed objectives are those that the development team has high confidence in delivering during the PI. Committed objectives are included in overall Business Value calculation.

Uncommitted objectives are used to identify work that can be variable within the scope of a PI. The work is planned, but the outcome is not certain. Teams can apply uncommitted objectives whenever there is low confidence in meeting the objective. This low confidence can be due to many circumstances:

Dependencies with another team or supplier that cannot be guaranteed.

The team has little to no experience with functionality of this type.

There are many critical objectives that the business depends on, and the team is already loaded close to full capacity.

Story (User Story)

Stories are short descriptions of a small piece of desired functionality written from the user's perspective. Agile Teams implement stories as small, vertical slices of system functionality that can be completed in a few days or less.

Stories are the primary artifact used to define system behavior in Agile. They are short, simple descriptions of functionality told from the user's perspective and written in their language. Each implements a small, vertical slice of system behavior. Stories provide just enough information for business and technical people to understand the intent. Details are deferred until the story is ready to be implemented.

Through acceptance criteria and acceptance tests, stories get more specific, helping to ensure system quality. User stories deliver functionality directly to the end user. Enabler stories bring visibility to the work items needed to support exploration, architecture, infrastructure, and compliance

2 Scope

(The PWS attached to this RFI serves as the base for multiple PWS. The Government will copy the base PWS and insert value stream-specific content in the Scope section and the Information on Historical Skillsets section. All other requirements are expected to be consistent across the Value Stream Agile Release Trains.)

This task order delivers and maintains functioning information technology products, services, and systems (applications) for the [insert value stream name here] value stream in support of its defined business objectives

and in alignment with ISD modernization goals. Information technology solutions must deliver future state as defined in the performance work statement.

Define value stream scope and identify clear boundaries here. If this value stream is closely related to or adjacent to another value stream, please define what is in-scope (part of this value stream) and out-of-scope (part of the other value stream). Sometimes defining what is not in scope can help us have manageable boundaries. (We want this definition now. If we have weak boundaries in the PWS, it will slow down later contract actions and create conflict.)

2.1.1 Value Stream Business Objectives

Objective 1:

Objective 2:

Objective 3:

Objective 4:

Objective 5:

Objective 6:

Objective 7:

2.1.2 Current State

The [insert name here] value stream includes but is not limited to the following active IT products, services, and solutions (applications).

Table 2. Current IT Products, Services, and Applications.

Application / System / Program Area	Support Activity

The value stream faces the following issues and concerns:

This is specific to functionality or solution stability/quality (measured in known defects).

This area is not describing what we like or don't like about service delivery today. Assume a blank slate as a new contract is awarded and comes in. Transition is covered in the Task area.

2.1.3 Future State

Describe the future state needed at the end of the contract. This is what we are holding the contractor accountable for achieving. Needs to reflect functional (business) and IT modernization.

3 Tasks

3.1 IT Solutions Delivery

The Contractor shall deliver IT solutions for approved, committed features meeting defined acceptance criteria and adhering to the standards of the FPAC Technology Governance Framework. The Business may decide not to release specific functionality, but the Contractor is required to deliver products or systems (applications) that are ready to be deployed to the Production environment.

3.1.1 Product Management Support

3.1.2 Requirements Management Support

FPAC Government Business Owners, Government Product Owners, and Government Program Managers leverage the Business Capability Roadmap and IT Modernization Roadmap to define solution-wide and product implementation plans. The Contractor shall provide and execute a plan within 30 days of contract start date explaining how the contractor will support maintenance and documentation of government-led product implementation plans throughout the product lifecycle to include product planning and implementation, product documentation, and product governance decisions. All product management processes must align to the FPAC Software Development Lifecycle and FPAC Technical Guidance Framework.

Government Product Owners continually define and refine business requirements within the value stream. Business requirements are stored in the government's designated requirements management tools, currently Atlassian Confluence and JIRA. Users or Government Product Owners may use science-based terminology to define requirements. The Contractor shall collaborate with Government Product Owners, Government Program Managers, and users from science-related-fields who may not have technological expertise. The Contractor shall provide requirements collection and analysis support to the Government Product Owner including business process modeling support, business requirements analysis, data analysis and models to represent data relationships accurately, business requirements documentation support, and architecture diagramming.

The Contractor shall support documentation and internal integrity of each government-led product implementation plan. At a minimum, product implementation plans identify and define program epics aligned to the portfolio epics in the Business Capability Roadmap. Program epics must be documented in the Government's designated requirements management tool and include (1) defined business outcomes and acceptance criteria, 2) a hypothesis statement and leading indicators, a complete description, attached documentation, (3) a backlog of approved program epics with linked dependencies (4) a time-phased implementation schedule by PI of the program epic backlog based on Government Product Owner prioritization, (5) requirements traceability across development and deployment phases for features and enablers, and (6) product documentation supporting the continued maintenance of work products.

The Contractor shall work with the Government Product Owner and Business Owners to translate business requirements into features and user stories which will be stored in the product backlog in the requirements management tool. Features are linked to parent program epics to demonstrate traceability to the parent program epic and portfolio epic. A feature shall be limited in size so that it can be fully completed within a PI. Government Product Owners must approve feature acceptance criteria before the Contractor begins implementation. A feature is broken into smaller pieces of value called user stories which contain a portion of value for the parent feature that can be fully completed within a two-week iteration. A user story defines the lowest level development requirement that is readily testable. The Government Product Owner retains the authority to prioritize the features within the Program Backlog. The Contractor shall increase collaboration as

necessary to effectively groom the product backlog, refine feature definition and details, clarify user-stories, estimate, identify dependencies, and establish understanding of acceptance criteria.

Deliverables:

A001 Product Management Strategy and Plan

A002 Product Backlog

3.1.3 Product Architecture

The Contractor shall create, document, and maintain product architecture meeting FPAC standards in performance, security, privacy, storage, processing, maintainability, reliability, dependability, recoverability, and that align with the FPAC Technical Guidance Framework. Product architecture encompasses computer systems, applications, and associated databases. Product architecture shall be flexible and able to integrate other applications or services and to enhance product features in accordance with standards in the FPAC Technical Guidance Framework. The Contractor shall perform system integration to unify the business application components with functions of other subsystems, develop and maintain interfaces to other business applications for the purposes of data sharing and dissemination, work with the infrastructure hosting provider to incorporate hardware and infrastructure components with business application and software designs to test newly developed software with existing components, develop software prototypes required for system design or capability analysis, and ensure improvements do not adversely affect ongoing operations.

FPAC Conservation has a 20+ year history of utilizing geospatial data in conservation planning activities that has evolved into the IT systems used today. Geospatial functionality and geospatial data integration now exist across most Conservation programs. NRCS business vision includes increasing and improving the integration of geospatial data resources across all Conservation areas. The Contractor shall architect and design applications with geographic information systems (GIS), improve geospatial functionality, and integrate geospatial data.

Software development includes creating software for, and interfacing with, mobile computing devices and any environments needed to support the FPAC IT Modernization Roadmap, including implementing computing services in a cloud environment. Table 3 provides a comprehensive list of major tools and technologies currently being used in support of this performance work statement.

Table 3. Major Tools and Technologies.

Category	Tool / Technology
IDE / Platform	Pega, MS Visual Studio, Eclipse, Angular JS, React JS, Adobe AEM, Drupal, AWS, Salesforce
Database	PostgreSQL, Oracle, MS SQL Server, MS Access
Language / Framework	Java, JavaScript, JSP, Servlets, JBoss, MS .NET, C#, React, Python, R Stats
Authentication / Authorization	zRoles, eAuth, SailPoint, Kerberos, LDAPT
Services	Postman, Swagger, SOA, Webservices (Custom built, Open domain, product specific)
Geospatial / GIS	ArcGIS, GeoTools, PostGIS, OSGEO, FME, GRASS, SAGA, Whitebox, R Studio Server

Category	Tool / Technology
Change Management / Code Repository	IBM Rational, Subversion, VSS, GIT, Bit Bucket, Docker
Repository	Jira, Confluence, SharePoint, MS Teams
Requirements Management	IBM Rational, Jira, Confluence
Web Servers	IIS, Tomcat, Apache, REACT
Deployment	DB Scripts, Jenkins, Liquibase
Compliance / Standards	Section 508, IT Security standards, WAI, NIST 800-53, FPAC SDLC, Geospatial Data Act, Federal Geospatial Data Committee, NARA,
Methodology	SAFe®, Agile, Maintenance
Reports	BIRT, MS SSRS,
Office Automation	MS Office
Operating Systems	MS Windows Server, Windows 10/11, RedHat Linux, Ubuntu
Testing	JIRA, Swagger, Ready API. Postman, ELK, IntelliJ, JAWS, NVDA, ANDI, Google Analytics, Cygwin Suite, Fortify, Axe DevTools, Selenium, Gauge, Color Contrast Analyzer, SonarQube, CyberArk

FPAC evaluates emerging and alternate technologies as needed to provide appropriate product lifecycle support. Such analyses may result in updates to the FPAC IT Modernization Roadmap and changes to product architecture. Agile solution and product architecture requires ongoing incremental analyses, some of which is very minor support to a product during migration, while other needs are larger. As many of NRCS's applications and systems are in the migration process and may need to be modernized or even decommissioned, the Contractor shall provide on-going architecture analyses and support and integration with the Solution Train. Contractors are required to be abreast of current and emerging technologies and have the capability to adapt to such emerging trends as required by the agency.

Deliverables:

A003 Product Architecture

3.1.4 Agile IT Solution Development

The Contractor shall commit to develop features by program iteration and sprint as prioritized and approved by the Government Product Owner and Government Program Manager. The process for this collaborative action is described in "Program-Wide Integration and Communication" (section 3.3). The Contractor shall identify and communicate all known dependencies outside its control prior to committing to a user story. If the Contractor identifies a dependency after committing to a user story, the Contractor shall notify the Government Program Manager by the start of the following business day. The Government will coordinate cross-organizational and cross-contract dependencies, committing to meet the dependencies per the approved sprint schedule.

The Contractor shall deliver IT solutions that meet the acceptance criteria of committed features and user stories per the approved sprint schedule. If a user story is not fulfilled and accepted by the end of the scheduled sprint, it must be delivered by the end of the PI. The Contractor shall design, develop, and test IT solutions using an iterative, Agile style that incorporates feedback from the Government Product Owner and other business and technical sources.

Application development includes end-to-end design, development, and testing of new applications and data systems supporting the agency mission as well as enhancing existing applications with new and modified features. Contractor shall support all such development initiatives and deliver solutions on platforms such as web and mobile devices as well as dedicated and cloud infrastructures. The Contractor shall integrate open source, COTS, Government Off the Shelf (GOTS) and/or SaaS solutions into existing, custom-built, or new systems and provide configuration, customization, and implementation services. The Contractor shall integrate with other government systems using modern standards-based communication protocols and data formats. The Contractor shall implement applications (web, thick and mobile) with other products and services such as web services extended for specific application(s) or available publicly, and Geographic Information Systems (GIS).

The Contractor shall increase test coverage continually per application using test driven development (TDD) and implementing a technical debt removal strategy. At a minimum, the Contractor shall automate unit testing for 80% of new code. The Contractor shall conduct testing as described in this performance work statement and provide results to ensure release of a quality work product.

The Contractor shall provide product and system documentation per the FPAC Technical Guidance Framework and FPAC Software Development Lifecycle. At a minimum, the Contractor shall generate comprehensive and complete documentation within the code itself and within the source code version control system (e.g., through proper use of descriptive commit messages, issue tracking, pull requests, etc.). As appropriate, the Contractor shall provide separate documentation, provide artifacts, and create new user stories based on each sprint.

The Contractor shall provide testing support, or automated equivalent, for the following unit testing, functional testing, deployment validation testing, integration testing, regression testing, performance and Load testing, and Section 508 of the Rehabilitation Act of 1973 testing for each software release.

The Contractor shall:

- Conceive, develop, document, and execute Test Plans for each system from development to production deployment.
- Develop and execute Test Cases for each system release to confirm technical specifications, business requirements, and dependent systems requirements have been fully satisfied.
- Perform software unit, system, and integration testing of software applications in accordance with the approved Test Plan and supporting Test Cases.
- Integrate security code review into the testing process.
- Perform full regression testing of each application whenever modifications have been made to the application that would require a full regression test. Regression Tests will be automated to the extent practicable, otherwise manual regression testing will be required.
- Develop and execute load and stress testing scripts using FPAC-approved performance testing tool.

At the end of each phase of testing, the testing results will be available in the FPAC designated requirements management tool. The tool will identify all issues found, resolved, and unresolved. The Contractor shall create the User Acceptance Testing process and protocol test plan. User acceptance testing is conducted by NRCS solely in the test environment.

Deliverables:

A004 Functioning IT Solutions

A005 Technical Debt Removal Strategy

A006 IT Solution Documentation

A007 Test Plans

A008 Test Cases

A009 Test Results

3.1.5 Deployment Planning and Readiness Testing

Deployments should not require any planned or unplanned downtime or outages, except to address extraordinary circumstances and pre-approved by the Government. The Contractor shall coordinate release planning in collaboration with other Conservation Program areas. The Contractor shall provide all documentation required for a successful deployment to and operation in production, including Government security and privacy assessments, release notes, and system help documents.

The Contractor shall develop release documentation including installation guide, operation guide, and network diagram. The Contractor shall plan, create, and validate application deployment scripts. The Contractor shall coordinate with the IT Operations teams to develop and deploy product packages which may include setting up servers and installing OEM products and patches. The Contractor shall provide additional documentation in support of audits, training, and application compliance, as required.

The Contractor shall perform Deployment Readiness Testing (DRT) under Government oversight to support the FPAC Quality Assurance process. DRT is limited to independent testing of applications by the development team for readiness or fitness to deploy to a production hosting facility. The kinds of applications to be tested will be web-enabled, deployed to a production hosting facility, and hosted in IIS/Windows or Apache/Linux computing environments. The length of time and resources required to perform testing and documentation will vary due to relative complexity of each project.

Prior to the Contractor performing the testing, the Government will provide to the Contractor the following Government-reviewed and approved items:

- Installation Package
- Installation and configuration document(s)
- Network Diagram(s)
- Test dataset required to run the application.
- Test environments including DNS, URL, Load Balancer, SSL certification, and a minimum of two virtual servers for testing.
- Functionality Test Scripts – Scripts for the testing whether an application runs properly once installed.
- The Contractor shall perform the following solely in the pre-production environment:
- Test the installation and configuration documentation by configuring the environment as described in the supplied configuration documentation and the supplied network diagram and installing the installation package according to the supplied installation instructions.

- Testing functionality of the application by running the supplied functionality test scripts.
- Test that the application works correctly under load balancers by the running the application under network load balancers.
- Test that the application is cluster aware – the application will recover after the application's database has been failed over to another physical node of the database cluster.
- Test the application's SSL requirement with an SSL hardware appliance and load balancer.
- Test the application with USDA eAuthentication http://www.eauth.egov.usda.gov/index.html if required by the application.
- Install and configure any required third-party COTS software.

After the testing, the Contractor shall:

- Provide a mark-up of the installation guide, configuration guide, smoke test procedure, operations guide, and network diagram noting any areas of confusion, error, or suggestions for improvement to the Government Program Manager.
- Post defects to the project's defect tracking system. Defects include issues, bugs, and documentation errors (see Table 4).
- If a test or certain step of a test failed, the Contractor shall document the test failure at the appropriate place in the test results. The Contractor is only responsible for deliverables in so far as tests can be executed.

The Contractor shall assist Government Program Manager with Release Readiness Review.

Deliverables:

A010 Release Plan and Documentation

A011 Deployment Test Readiness Results

3.1.6 User Training and Customer Support

The Contractor shall develop and implement comprehensive training materials to support user adoption of IT solutions. Training materials may include documentation, standard operating procedures, demos, and recordings (e.g., Microsoft Teams recorded tutorial). The Contractor shall support user training and ensure that the IT Operations team has the information, training and system access required to provide successful customer support. The Government will define user training requirements and acceptance criteria via the product backlog. The Contractor is required to provide reach back support for the Service Desk and Operations team(s) for Tier 3 requests.

Deliverables:

A012 User Training Materials

A013 Service Desk Training and Reference Materials

A014 Tier 3 Resolution

3.1.7 Optional CLIN: Additional Requirements within Value Stream Scope

Insert content here about potential for additional capacity up to 50% of initial scope.

3.2 IT Solution Maintenance

The Contractor shall maintain all active IT products, services, and applications. Application maintenance includes:

Preventive maintenance – These are activities that are done proactively for the purposes of preventing problems before they occur. Activities include but are not limited to:

- Applying appropriate and latest software upgrades and patches,
- Monitoring the health of application systems and performance,
- Continuously support availability of application systems, and
- Provide audit mediation support and testing of applications to determine if audit findings have been resolved and addressed.

Corrective maintenance – These are activities that are performed to correct defects / issues in the application environment (hardware, software, application, sub systems, etc.) to maintain current functional and non-functional features of the application system(s). Examples include but are not limited to:

- Triage issues reported and work in collaboration with Government staff in prioritizing and classifying the issues and defects recorded,
- Record issues and defects reported by the stakeholders in the approved software tool,
- Develop work around emergency deployments
- Fix and test application code, batch jobs, bugs, and databases,
- Verify fixes and continuously monitor system to ensure no residual defects due to fixes,
- Acknowledge resolution of reported issues within the stipulated SLAs, receive feedback, and close reported issues on resolution,
- Report defect and issue application-wise status periodically and as requested, and
- Maintain a knowledge base on all defects / issues reported,

Adaptive maintenance – These are activities that are performed to sustain operations and availability of application systems in response to environment changes such as hardware upgrades, OEM releases, technology changes, audit findings, new or modified web services, security concerns, etc. Activities may lead to implementation of new minor features. Activities may include but are not limited to:

- Support changes to database structure, data quality control, data integrity and other best practice data management activities,
- Provide data repository administrative support services, management, and maintenance (e.g. COLAB); excludes licenses purchases, and
- Implement agility and support prioritized initiatives by the agency that may involve reorganization of develop team and switch to a different technology platform as necessary.

Perfective maintenance – These are activities that are performed to ensure performance and maintainability of application systems and improve efficiencies. Activities include but are not limited to:

- Code refactoring/ optimization, database maintenance and implementing certain minor application features,
- Support for updating legacy applications to contemporary coding standards, languages, and technologies, and
- Research, lead, or participate in studies and collect, analyze, and integrate information to identify and address problems or issues.

In addition, application maintenance includes:

- Maintaining all source code, application files, and associated documentation in the agency designated version control system,
- Administering consistent use of tools and repositories supporting software and system delivery and maintenance, and
- Supporting formal decommissioning of applications according to USDA OCIO and FPAC disposal and decommissioning guidelines and plans to include documenting the entire process.

In addition, the Contractor shall ensure USDA disaster recovery sites replicate production application code and data. The Contractor shall participate in planned and unplanned disaster recovery/continuity of operations (COOP) exercises. In the event of an emergency, the Contractor shall execute disaster recovery and COOP plan in coordination with the Government.

Table 4 defines the defect levels applied to defects found during user acceptance testing and in production.

Table 4. Defect Levels.

Security Level	Urgency	Description	Examples
0	Section 508 Legislation Compliance	Used to identify defects that are related to Section 508 Compliance (Section 508 of the Rehabilitation Act of 1973)	Defects/Failures identified by automated test tools. Defects/Failures identified by running manual test cases.
1	Blocker	An issue that affects a requirement for which there is no workaround. It prevents either use or testing of the system.	Defects/Failures causing unavailability of system or functionality.
2	Critical	Testing cannot proceed until the defect has been corrected. The defect is critical enough to: crash the system,	Defect causing downstream impact to other applications. For example, a document for a producer is selected in Conservation Desktop but the wrong Core Customer ID is sent to Farmers.gov making the document unviewable or signable.

Security Level	Urgency	Description	Examples
		cause file corruption, or result in potential data loss. It causes an abnormal return to the operating system, i.e., either a crash occurs, or a system failure message is generated. The defect causes a program to hang, requiring that the system be re-booted. It results in a lack of vital program functionality for which there is no work-around.	Defect on data calculation required for a conservation resource assessment that returns the wrong value or does not return a value (data loss). Defect on Conservation Desktop logon in which the system locks up or crashes.
3	Major	Although it is unlikely the defect will cripple the system, it does create severe problems, e.g., serious formatting errors, etc. The lack of functionality resulting from the defect presents major inconvenience to system users. A work-around exists for the problem, but implementation of that work-around is difficult, complex, and/or inconvenient. An insufficient or unclear error message appears, resulting in a major negative impact on product use. The defect prevents other areas of the product from being tested.	A user is unable to work in Conservation Desktop until the customer's casefile lock is released in ProTracts Application. Defect on electronic signature for a document in Conservation Desktop requiring the user to print the file to manually sign scan and re-upload the document into the Document Management System.
4	Moderate	While serious in nature, the defect is less severe than a major problem. A simple work-around for the problem exists. An insufficient or unclear error message appears but results in minor negative impact on product use.	Defect where function should behave a certain way but doesn't, but the end user can take a different path (within reason to complete the function. Defect where error message is meaningless to end user.
5	Minor	The defect is primarily a cosmetic issue.	Spelling or punctuation error.

Security Level	Urgency	Description	Examples
			Formatting change would improve display and usability.
6	Enhancement	The defect is a suggestion for improving the application.	Improvement to user experience that is not covered in user requirements or acceptance criteria.

Deliverables:

A015 Software updates and fixes

A016 Revised software documentation

3.3 Program-Wide Integration and Communication

To ensure effective NRCS program delivery, the Government defines and oversees a common delivery cadence across all components of Conservation IT service delivery. The Contractor shall adhere to the coordination, integration, and communication requirements described in this performance work statement in support of the common delivery cadence.

3.3.1 Coordination and Collaboration

The Contractor shall coordinate with multiple stakeholders across the Conservation team including the Government Business Owner, Government Product Owner, Government Program Manager, other business and technical federal stakeholders, and other federal and contractor teams. FPAC requires all parties to work alongside each other in a collaborative environment creating a quintessentially gray badge environment. We are all part of one team supporting NRCS mission delivery. The Contractor shall embody a highly collaborative and cooperative attitude to enable positive interaction with the Government and other Contractors to avoid duplication of effort and to ensure the coordination of work efforts.

The Contractor shall coordinate with the Solution Train to plan, align efforts, and provide accurate and verifiable metrics during pre-planning, PI planning, and PI execution. The Solution Train team, with Government Program Manager and COR approval, may establish or try-out common measures, standards, guardrails, or capacity forecasting methods across all ARTs. The Contractor shall adopt and support these portfolio-wide efforts. Coordination between the Solution Train team and each ART's Release Train Engineer must support scrum masters, product owners, and business owners identifying, grooming, prioritizing, and approving user stories to define the work performed during a PI.

The Government Business Owner and Government Program Manager provide guidance on the vision, requirements, and priority of work and validate the delivered IT solution meets the acceptance criteria as defined in the PI plan. The Contractor Program Manager shall work closely with the Government Program Manager. The Government Program Manager provides technical oversight in close coordination with the COR who provides contract oversight. The Contractor shall NOT take technical direction related to deliverables or services under the PWS from anyone other than the Government Program Manager in concert with the COR. Only the Contracting Officer may adjust contractual terms and conditions including changes to deliverable

definitions, acceptance of non-compliant deliverables, consideration for potential government delays, and invoice schedule changes.

The Contractor Program Manager and Release Train Engineer are responsible for managing issues and impediments for/within all teams within the ART including establishing an escalation path for the ART. The Government recommends but does not direct the following escalation path:

- Person to Person
- Person to Scrum Master
- Person to Release Train Engineer (RTE)
- Person to Agile Coach
- Person to Solution Train Engineer (STE)
- Person to Contractor Program Manager
- Person or Contractor Program Manager to Government Program Manager (GPM)
- Contractor Program Manager and/or Government Program Manager to COR

3.3.2 Program Cadence and Synchronization

Conservation IT service delivery leverages Scaled Agile Framework (SAFe) principles and organization. Portfolio-wide planning uses a common delivery cadence consisting of synchronized iterations and PIs. The Government defines the portfolio-wide iteration schedule with input from contractors. The program of work is segmented into 12 or 14-week PIs (PI) consisting of five or six 2-week development iterations and one 2-week Innovation and Planning Iteration. PIs and iterations are synchronized across teams by aligning the teams' schedule. The PI and Iteration schedule is coordinated by the Solution Train Team.

3.3.2.1 PI Planning

During the last iteration of a PI, the Contractor shall meet with the Government and other Conservation Program components to plan the next PI. This event is referred to as PI Planning, or PI Planning, and usually occurs over a four-day period with a fifth day for the Solution-level sync. The Government will provide a list of prioritized features that are fully defined with acceptance criteria. The Contractor development teams shall plan the delivery of the features collaboratively with the Government Product Owner(s). The teams will plan to deliver functioning software or systems by implementing the features through user stories during the first five iterations of the upcoming PI. The last iteration, known as the Innovation and Planning Iteration, is reserved for the next PI Planning session and application maintenance activities such as defect fixes, refactoring code, implementing infrastructure enablers, innovation spikes, etc.

3.3.2.2 Features, User Stories and Relative Estimating

In preparation for PI Planning, the ART scrum teams define and prioritize features and estimate the size of each feature using relative estimation. The Contractor shall decompose features into user stories, an activity that may occur prior to PI Planning or during PI Execution. The Contractor shall provide a feature and user story sizing and prioritizing methodology that follows the standard Agile and SAFe® practice of using relative estimates generated by the team and captured in story points by assessing the quantity of work, the work complexity, the degree to which the solution is known, and the amount of uncertainty contained in features and user stories during PI planning and confirmed in sprint planning. Point estimation must be normalized across an ART's teams so that as estimates roll up into features, the ART has a shared basis for economic decision-making. Prior to estimation, the Contractor shall work with the Government Product Owner to capture sufficient detail of the features and

stories, so the team can estimate the story points, but not so much detail that it stifles the conversation surrounding the features and stories.

3.3.2.3 Program Increment Plan and Business Objectives

During PI planning, the Contractor shall coordinate with the Government Business Owner and Government Program Manager to create a PI Plan that identifies features to be completed during the PI and dependencies with the Government, other contractors, and external parties. The features that the teams plan to deliver during the PI will be captured in the Team Backlog within the FPAC requirements management tool. In addition to planning the iterations, the teams shall coordinate dependencies with each other and external parties.

Team capacity per iteration is an estimation of a team's capability to perform and deliver value. The Contractor shall define the PI Plan based on adjusted team capacity. Adjusted team capacity considers factors such as resource availability (holidays, leave schedules) and guardrails to promote quality and address emergent O&M needs. The Government historically used 10% of team capacity as a guideline, but the Contractor shall establish appropriate guardrails to ensure delivery of functioning software features at the end of the PI per the Government's program delivery deadlines.

Team velocity is a measurement of demonstrated performance from previous iterations. The government recognizes that velocity is a backward-looking metric, is exclusively owned by each development team, and provides the team itself and the Product Owner with an indication of how much work can be done within one Sprint (for that specific team). The Government will consider team velocity trends (increasing, maintaining, or decreasing) when assessing risk to product delivery schedules.

After the teams fully allocate their capacity for the PI with features, the teams shall create a list of Business Objectives that shall be achieved when they deliver the planned features. A business objective may be comprised of multiple features. The teams will then commit to delivering those business objectives at the end of PI Planning. Teams shall designate any objectives that contain a lot of risk or uncertainty as uncommitted or stretch objectives. The business owners or their designees shall assign a business value to each objective, representing the relative value of the objective to the business. The list of committed team objectives and uncommitted team objectives and their corresponding business values are a deliverable to the government at the end of PI Planning in the form of a document or power point slide with the associated features and program epics documented in the Government's designated requirements management tool.

During PI Planning, the Contractor and the government shall identify risks to successfully delivering the objectives for the PI. The Contractor shall work collaboratively with the government on risk management until each of the risks are Resolved, Owned, Accepted, or Mitigated (ROAM' d).

At the conclusion of PI Planning, the Contractor shall deliver a PI Plan including (a) adjusted capacity by team, (b) list of features to be delivered, (c) dependencies, (d) risks, and (e) backlog of committed and uncommitted business objectives with associated business values. The Contractor shall document backlog features, epics, and objectives in the Government's designated requirements management tool.

Deliverables:

A017 Program Increment Plan

3.3.3 Program Increment Execution

3.3.3.1 Iteration Planning

Iteration planning will be performed at the beginning of each iteration, in collaboration with the Government Product Owner. At iteration planning, the teams shall ensure that features are being completed according to the

approved acceptance criteria and review the program epics completion status. The approved features for the PI will be decomposed into user stories. The Contractor shall commit to user stories to be delivered during the iteration in accordance with the capacity estimation methods. The committed User Stories shall be contained within the Team Backlog and Iteration Boards in the FPAC requirements management tool.

3.3.3.2 Iteration Demonstrations

At the end of each iteration, the Contractor shall demonstrate the work performed against the feature and story acceptance criteria during the iteration to the Government Product Owners. In the event the Government Product Owner desires changes or additions to the work performed and demonstrated to achieve the business value for the features and objectives, the change shall be managed by adding the changes required to the Program Backlog and prioritized accordingly for the next iteration and/or increment. The iteration demonstration and approval of features demonstrates evidence of progress towards feature delivery.

3.3.3.3 Iteration Retrospectives

Each iteration, the teams shall perform a team retrospective for the iteration. The teams shall identify what processes worked well and should be continued. The teams shall also identify which processes did not work well and should be improved.

3.3.3.4 Feature Demonstrations and Acceptance

The Contractor shall perform system demonstrations to the Government Business Owner, Government Product Owners, Government Program Manager, and COR on a biweekly basis during the PIs. These system demonstrations will be focused on demonstrating completed features. The government can choose to accept the feature using the acceptance criteria or request changes to the work performed to achieve business value. Feature acceptance by the government shall be designated by a change to the status of the feature within the FPAC requirements management tool. In the event the Government Product Owner desires change to the work performed and demonstrated, the change will be managed according to the change control process outlined in this performance work statement.

3.3.3.5 Deployment Readiness and Decision

The Contractor shall coordinate with the Government Product Owner, Government Program Manager, Security Engineering and Assessment Team, Assessment and Authorization Team, and Production Support Operations Team to determine if a release is ready to be deployed. The Government seeks to increase the release cadence to deploy features at the end of each PI to the extent practicable.

3.3.3.6 Handoff from Development to Operations

The scope of Conservation Software Delivery spans development, delivery, and operations and maintenance application support for Conservation Mission Delivery applications. The scope of the services shall include Production Systems Operations support, Non-production Operational support, Infrastructure support, Platform Support, CI/CD Pipeline support, or Service Desk Support. It is expected that the teams will actively support the excellence of these efforts and work collaboratively. While supported by separate contracts and distinct teams, lines will be blurred at times due to the nature of DevOps. The Government expects all teams to work together towards the common goal.

Development: “Stream-Aligned Team” (Mission Delivery/Development team)

Operations: “Platform Team” (DevOps Core team)

The scope of the PWS includes coordination between the Development team(s), the Operations team(s), and Security teams including coordinating with and across all Operations’ activities and functional areas.

3.3.3.7 Inspect and Adapt Sessions

At the end of each PI, the Contractor shall host Inspect and Adapt sessions to demonstrate the features delivered to the government and perform continuous improvement. The Contractor shall coordinate with the Solution Train Team.

3.3.3.8 Full IT Solution Demonstrations

During the Inspect and Adapt Session, the Contractor shall support IT solution demonstrations to the government highlighting the work performed that delivered the features defined within the previous PI Planning Event. The demonstrations are to be “live” applications performed within an integrated environment. The live Inspect and Adapt demonstration provides evidence of functioning software delivery.

3.3.3.9 Quantitative Assessment

During the Inspect and Adapt session, the business representatives shall score the business objectives based upon how much of the total business value was achieved and demonstrated in the system demo. The business value Achieved from objectives and stretch objectives (summed) divided by the total Planned business value sum from committed objectives defined and scored during PI Planning equate to a total achievement percentage. The Contractor shall average at least a 90% (or above) total achievement percentage at the end of each PI. If the Contractor does not meet that total achievement percentage in each PI, the Contractor must deliver a plan for improvement to the government by the end of the next iteration. If improvement is not recognized in the PI after that plan for improvement is implemented, the Contractor shall receive a written notice from the contracting office that improvement is required. If a secondary failure to meet the 90% total achievement percentage occurs, the government may terminate the contract for failure to comply or withhold full payment until rectified by the Contractor. The quantitative assessment and metrics scoring are a deliverable to the government within a week after the Inspect and Adapt Session.

3.3.3.10 Program Increment Retrospective

At the end of the Inspect and Adapt Session, the Contractor shall conduct an overall PI Retrospective to identify processes to improve and problems to solve. Action items from this session will be added to the program backlog for future consideration. The PI retrospective is a deliverable to the government in the form of a document or power point at the end of each PI within 1 week after the end of the PI retrospective.

Deliverables:

A018 Iteration Demonstrations

A019 Feature Demonstrations

A020 Full IT Solution Demonstration

A021 Program Increment Retrospective

3.3.4 Change Control Process

The SAFe agile process uses incremental development and regular feedback to ensure user needs are met and business value is achieved. As a result, changes are allowable with approval architecture guardrails and available team capacity. Changes may occur prior to PI planning, after PI planning, or upon demonstration of delivered user stories or features.

3.3.4.1 Changes to specifications prior to PI Planning

If the government needs to make changes to feature definitions prior to PI Planning, the change is fully accepted and allowed. The feature must be defined with acceptance criteria by the approval of the PI Plan to be considered for development during that PI.

3.3.4.2 Changes to specifications of committed objectives after PI Planning

If the government needs to make changes to specifications after the feature/functionality has been committed to at PI Planning or change priorities due to more urgent business value needed, the teams will assess the impact to the teams' capacity to deliver the newly defined functionality. If the effort to implement the change exceeds the ability to complete the work along with the rest of the teams' commitments, the Contractor will meet with the Government Program Manager, Government Product Owner, and Government Business Owner to determine which objectives are still achievable, and which commitments the teams need to be released from to deliver the modified feature/functionality. These changes will be reflected in specific notations in the PI Plan about business value delivered and which objectives were not achievable. The Contractor shall not execute changes to the PI Plan prior to receiving concurrence from the Contracting Officer's Representative.

3.3.4.3 Changes to specification of work in progress or work performed.

If the government needs to make changes to specifications after work has been performed on a feature/functionality, the newly defined feature/functionality will be added to the team or program backlog. If the change is required to deliver the feature, the teams will assess the impact to the teams' capacity to deliver the newly defined functionality. If the effort to implement the change exceeds the ability to complete the work along with the rest of the teams' commitments, the Contractor will meet with the Government Program Manager, Government Product Owner, and Government Business Owner to determine which objectives are still achievable, and which commitments the teams need to be released from to deliver the modified feature/functionality.

If the requested change does not affect the teams' ability to meet commitments for the current PI, and is suitable for development within future PIs, the newly defined feature/functionality will be added to the Program Backlog for future consideration and prioritization by the government.

3.3.5 Continuing Maturity

Immediate success hinges on both maintaining the current "status quo" and continuing to push the current forward-looking efforts and enablers. Many efforts are underway in almost every area of development to move FPAC forward to a higher DevOps maturity, but FPAC does have many legacy applications with significant technical debt. This leads to complex situations that need careful planning and attention to detail to navigate successful deliveries.

All development within Conservation uses agile methodologies at varying scaled levels. On the larger efforts, Conservation is entering its twenty-eighth PI using the SAFe® methodology. FPAC is continuing to mature and is making changes to move to a more frequent release schedule, a higher level of quality through fully automated testing/deployments, and end to end tracing of requirements.

The current state is a mixture of great successes while facing the challenges of lagging technical debt. Our goal is to continue along the learning curve with more successes in the areas of DevOps, CI/CD, TDD/BDD, UCD, smaller more frequent releases, and other focus areas. All of these have one end goal – Quicker, high-quality delivery of value to the internal and external customers we serve.

3.4 Transition

3.4.1 Transition In

Onboarding and knowledge transfer are necessary activities to ensure continuity of program delivery for the Government and to prepare the incoming contractor for full performance. During transition in, the focus is on knowledge transfer to understand the existing and expected Conservation environment and to solidify program integration and communications. The Contractor is not required to meet all performance standards in the performance work statement during the transition in period. The Contractor shall provide all required services and meet acceptable quality levels beginning the date of full performance identified in the contract award. One week prior to the end of the transition in period, the Contractor shall schedule a Full Performance Kickoff Meeting. At a minimum, the agenda will include:

- Status of key personnel readiness,
- Train readiness by team,
- Review of product backlog status, and
- Discussion of performance, schedule, and other risks with mitigations.

3.4.1.1 Onboarding

The government onboarding process with expected timeframes is included within the “Onboarding Process” Attachment x. FPAC will host a government onboarding kickoff meeting within one week of award and will initiate the government onboarding process with the Contractor. Onboarding packages need to be submitted as soon as possible, with an initial turn-around target of four business days following the onboarding kickoff meeting or from date of hire during contract performance.

Incoming contract resources may begin interacting with the Government and incumbent personnel for knowledge transfer upon receipt of the security initial determination (SID). Incumbent contract resources (moving to new contract via incumbent capture) may continue to work under an existing SID while they are undergoing the onboarding process for receiving a new SID under their new contract number.

FPAC estimates the average time to complete the FPAC onboarding process to be 4 - 8 weeks. The timeframe to obtain a SID varies based on several factors. No other government personnel are privy to reasoning behind an unfavorable SID.

Each Contractor is required to utilize a Personal Identity Verification (PIV) card to access IT systems and Sensitive Information. Using shared accounts to access IT systems and Sensitive Information is strictly prohibited. USDA/FPAC may disable accounts, and access to IT systems may be revoked and denied if Contractors share

accounts or allow Information Security Awareness Training certificates to lapse. Users of the systems will be subject to periodic auditing to ensure compliance with USDA and Agency policies. Each Contractor is required to utilize Government furnished equipment.

3.4.1.2 Knowledge Transfer

Both the incumbent and incoming Contractor, as soon as possible, shall use the government's designated tools to capture and transition information, artifacts, products, and knowledge.

Contractor resources must participate in knowledge transfer meetings, communications, and activities with the Government and incumbent contractor immediately upon receipt of an acceptable security initial determination from the Government. Knowledge transfer may occur in parallel with continuing onboarding activities, such as receiving Government furnished equipment and access to Conservation environments. The Contractor shall work with the Government Program Manager to coordinate meetings with Government stakeholders and the incumbent contractor.

The Contractor must provide transition-in/knowledge transfer status updates to the government, at a minimum weekly, throughout the transition in period.

Deliverables:

A022 Transition In Reports

A023 Full Performance Kickoff Meeting

3.4.2 Transition Out and Knowledge Transfer

Transition-out efforts will focus mainly on knowledge transfer about the current work agreed to and any work planned or underway. Transition out is expected to occur during the final PI.

No later than 45 calendar days prior to the start of the final PI, the Contractor shall provide a preliminary knowledge transfer plan for all deliverables, products, and materials in coordination with the COR, Government Program Manager, and Government Business Owner from FPAC. The Government will provide feedback within two (2) weeks.

A final Transition Out Plan is due to the government no later than 14 calendar days prior to the PI Planning event for the final PI. Both the incumbent and incoming Contractor, as soon as possible, will utilize the government's designated tools to capture and transition information, artifacts, products, and knowledge.

The Contractor must provide transition-out/knowledge transfer status updates to the government, at a minimum weekly, throughout the final PI. A Transition Out Report shall include a list of sprint tasks completed, documentation, and link to code repository developed for Conservation five (5) days prior to the end of the contract. Should the Contractor be terminated prior to the end of the period of performance, the Contractor shall transfer all project materials to the COR (and/or other COR-designated government POCs) within two weeks of the COR's request. The final Transition Out Report is a contract deliverable.

During the transition the Contractor shall perform all necessary transition activities, including, but not limited to:

- Develop transition plan including transition approach, communication, and performance criteria.
- Continue to provide full services to the Government,

- Participate, at the discretion of the COR, in recorded meetings with the Government or new contractor to support a smooth transition and provide detailed information on program management services, deliverables, and supporting materials,
- Perform knowledge transfer to new personnel (contractor or government) during the transition period,
- Complete any necessary documentation as requested by the program manager, COR, or other government employee,
- Provide availability to answer any questions that arise, and
- Provide information such as source materials, collaborative work products, government feedback, and contract deliverables that should be available to the Government in the collaborative workspace established from contract's initiation. Should the contract be terminated prior to the completion of all deliverables, the Contractor shall work with the Government to ensure the Government retains access to this information within two weeks from the termination date.
- Ensure and agree that all deliverables, products, licenses, designs, data, documentation, tests, user research notes, source code, configuration settings and files, and materials developed throughout each PWS will be the property of the U.S. Government.
- Coordinate with the COR and potentially another Contractor and implement the Transition Plan.
- Assist the COR, Product Manager, and potentially other Government staff to stand-up any applications developed during the PWS.

Transition-out activities may occur with Government personnel, an incoming Contractor, and/or another 3rd party. The Contractor shall coordinate with all parties to ensure a seamless and effective transition.

Deliverables:

A024 Transition Out Plan

A025 Transition Out Reports

3.5 Task Order Administration

3.5.1 Program Management

The Contractor shall provide overall Project / Program Management support apart from implementation teams to manage and deliver periodic reporting on project and product status, resource utilization, planning, value delivery metrics, overall program level documentation required for the agency and department, and issue resolution. At a minimum project management support shall:

- Assess staffing needs,
- Address mandatory training requirements,
- Address how Contractor will quickly pivot to support a new business requirement that requires a new/different skillset,
- Validate personnel skillset(s) and provide the adequate level of expertise,

- Staff for on the first day of full performance based on the current and future state described within the PWS, and
- Ensure staff has the expertise, knowledge, and familiarity with the current state to perform on the first day of full performance.

Conservation is a complex area with demands from multiple agencies and active political oversight. Demands for functionality come fast and furious, often requiring compromise. Demands can be driven by legislation or the USDA or NRCS strategic vision. The combination leads to a dynamic environment. Conservation programs are implemented using SAFe® as the primary methodology. Due to the level of investment, the delivery team may find itself in a situation where time, cost, and/or scope are all fixed. Tolerance to defects is low and stakeholders are willing to invest in quality, but some timelines are short, and delays are not well received. Reporting and status expectations are extremely high with root cause analysis and justification for issues even higher. The resulting expectation of performance is very high and significantly subjective. Contractor program leadership must be well versed in dealing with all aspects illustrated above.

3.5.2 Kickoff Meeting

The Contractor shall coordinate with the Contracting Officer and COR to schedule the task order kickoff meeting. The Government will review the performance work statement during the contract kickoff meeting. The task order kickoff meeting agenda will be divided between the Government and the Contractor. At a minimum, the Government will introduce the Government's team and review the performance work statement, key contract terms and conditions, and the FPAC contractor onboarding process. At a minimum, the Contractor shall introduce the Contractor's program management team and key personnel and review the staffing, onboarding, and training plan with anticipated timelines, templates for reporting deliverables, and task order knowledge management plan. The Contractor shall provide meeting minutes five (5) business days after the meeting.

Deliverables:

026 Task Order Kickoff Meeting

3.5.3 Training and Knowledge Management

The Contractor shall ensure their employees (including subcontractor personnel) complete the training course(s) listed below in the frequency identified. The contractor must maintain records of course completion and provide them to the Contracting Officer or Contracting Officer Representative upon request. The Contractor shall develop and implement a knowledge management plan including the development and maintenance of comprehensive training materials to support knowledge transfer within the Contractor team and ensure continuity of operations with negligible impact on productivity. Training materials may include documentation, standard operating procedures, demos, and recordings (e.g., Microsoft Teams recorded tutorial). The Government may leverage available training materials if new Government team members are introduced.

Table 5. Required Contractor Training

Course Name	**Frequency (once, quarterly, annually, etc.)**	**Method of Training**	**Length of Training**	**Completion Date**

Understanding and Interrupting Unconscious Bias	Annually	AgLearn	90 minutes	90 days after assignment in AgLearn
Anti-Harassment Training: Identifying and Preventing Workplace Harassment	Annually	AgLearn	60 minutes	90 days after assignment in AgLearn
Information Security Awareness	Annually	AgLearn	60 minutes	1 year since last completion date
USDA Records Management	Annually	AgLearn or paper-based	60 minutes	60 days after assignment
Section 508	Annually	AgLearn	60 minutes	45 days after assignment

Deliverables:
A027 Knowledge Management Plan

3.5.4 Reporting

3.5.4.1 Contract Roster

Immediately following contract award and annually, the Contractor must provide the Contracting Officer's Representative with a complete list of employee names, date of SID, and date of current FY year completion of USDA Information Security Awareness Training. Information Security Awareness Training completion certificates are maintained in AgLearn.

3.5.4.2 Status Reporting

The Contractor shall deliver reporting on project/product status, resource utilization, planning, value delivery metrics, overall program level documentation required for the agency and department, and issue resolution at the completion of every two iterations, to coincide with invoice submission. The Government may request status briefings at least weekly.

Status reports shall contain the following information for the task order:

- PI status in color-coded (green/yellow/red) status with reason for yellow/red status,
- Staffing levels with onboarding status,
- Current train capacity metrics,
- Key tasks accomplished,
- Ongoing and upcoming releases with release milestone progress.

Status reports shall contain the following information at both the Train and Team level:

- Story status metrics with dashboard visualization,
- PI iteration metrics on features/enablers planned vs accepted, such as stories planned vs accepted, % stories accepted, stories moved to next iteration, story points planned vs accepted, rolling average velocity, velocity change, % accepted, % fallout, target % acceptance, business story points planned vs accepted, enabler story points planned vs accepted,
- PI iteration quality metrics, such as MCB defects found, MCB defects closed, MCB defects open, escaped/deferred defects, defect trending,
- O&M quality metrics in Production, such as MCB defects found, MCB defects resolved, MCB defects open, escaped/deferred defects, defect trending,
- Delivery velocity (story points per PI) trending,
- Risk/issue register reporting on train-level risks/issues opened, in-progress, and closed during the PI.

The Contractor shall submit a visual dashboard snapshot of these metrics, along with a link to source data in Jira. As applicable, the Contractor must be able map each Team with a team's Committed Business Objectives, and Actual Achieved Business Objectives at the end of a PI.

3.5.4.3 Invoice Supporting Documentation

The Contractor will invoice in accordance with completion of an iteration or multiple iterations, approved by the government (COR/CO). The Contractor must have a designated POC that maintains funding obligations and amounts invoiced. The Contractor Financial Tracking POC must be available to work closely with the COR, or other designated government personnel to, at a minimum:

- Organize how invoices will be entered into IPP,
- Align and provide summary of Contractor work delivered each sprint/iteration and include invoice supporting backup documentation,
- Track contract obligations,
- Forecast FFP expenditures by planned iterations,
- Forecast additional funding needs or surge expectations,
- Track invoice payments by IPP WBS-code or funding distribution line item (if needed).

Each invoice will align to work completed and/or work delivered at the end of an iteration. Government acceptance of an invoice will be based on the agreed upon performance standards in the performance work statement.

The NRCS product backlog includes projects approved by the NRCS IT governance framework (e.g. Investment Review Board (IRB)). NRCS must capitalize all internal software development projects costing $500,000 or more. Operations and maintenance costs are not capitalized. Each invoice will include supporting documentation identifying the applications supported by team with a percentage of capacity spent on each application and O&M. O&M may be reported as a single number for all applications supported.

Deliverables:

A028 Contract Roster

A029 Status Reports

A030 Invoice with Supporting Documentation

3.5.5 Quality

The Contractor shall develop a quality control plan (QCP) and maintain an effective quality control program to ensure services are performed in accordance with the performance standards contained in this PWS. The Contractor shall develop and implement procedures to identify, prevent, and ensure non-recurrence of defective services. The Contractor's QCP is how the Contractor assures work complies with the requirement of the contract. The finalized QCP will be accepted by the Government at the time of the award. The Contracting Officer may notify the Contractor of required modifications to the plan during the period of performance. The Contractor then shall coordinate suggested modifications and obtain acceptance of the plan by the Contracting Officer. Any modifications to the QCP during the period of performance shall be provided to the Contracting Officer for review no later than 10 working days prior to effective date of the change. The QCP shall be subject to the Government's review and approval. The Government may find the QCP "unacceptable" whenever the Contractor's procedures do not accomplish quality control objective(s). The Contractor shall revise the QCP within 10 working days from receipt of notice that QCP is found "unacceptable." The Government shall monitor the Contractor's performance under this contract in accordance with the Government's Quality Assurance Surveillance Plan (QASP).

Deliverables:

A031 Quality Control Plan

3.6 Contractor and Key Personnel

All contractor personnel shall collectively possess professional proficiency, experience, knowledge, and skills to perform all required tasks. The Contractor shall ensure that its staff and subcontractors maintain any required professional certifications, accreditations, and proficiency relative to their areas of expertise. The Contractor shall make every effort to retain personnel and ensure continuity, continuous value delivery, meeting business needs, and establishing competency until contract completion. The Contractor must maximize productivity and minimize attrition.

If the Contractor makes changes mid-PI that have an impact on PI commitments (e.g., the effort to implement the change exceeds the ability to complete the work along with the rest of the teams' commitments) the Contractor will meet with the government product manager(s) to determine which objectives are still achievable, and which commitments the teams need to be released from to deliver the modified feature/functionality. The Contractor PM is responsible for informing the COR if the following trends start to occur: the Contractor continues to implement changes that negatively impact commitment to PI objectives, and/or features or stories repeatedly spillover.

The GPM and Contractor PM are responsible for communicating to the COR whether Contractor-owned changes are an acceptable byproduct of agility, failing fast, and recovering quickly vs. Contractor team misalignment or mismanagement. Contractor-owned changes and impacts must be tracked and documented. Any reports of Contractor mismanagement or misaligned teams may be reported by the COR as an issue in the category of "Management and Business Relations" within the Contractor's Performance Assessment Ratings (CPARs).

The Contractor shall ensure continuity of operations during periods of personnel turnover or a long-term absence, with minimal impact to a team's velocity and team commitments. The Contractor's performance ratings will include assessment of team member attrition.

The Contractor PM is responsible for providing a complete staffing list to the COR on a regular basis, at least monthly, as a contract deliverable. The Contractor PM is also responsible for discussing individual team velocity (or baseline capacity) with the COR on a regular basis. The COR and Contractor PM are jointly responsible for verifying that the Contractor maintains the proposed level of effort for each fixed-price team. The COR and Contractor PM are jointly responsible for communicating and documenting risks of performance issues, foreseen impacts to team velocity, or any other disruptions (that may or may not be caused by Contractor Personnel).

3.6.1 Contractor Program Manager

As a part of the critical path to success, the Contractor Program Manager (PM) is required key personnel. The Government expects that the PM be dedicated for the duration of the period of performance.

The Contractor PM shall be a single management focal point to accomplish the administrative, managerial, and financial aspects of this PWS. The PM will serve as the primary point of contact for all contractual or programmatic Issues. The PM will provide qualified team staffing, timely problem resolution, regular reporting in accordance with program management methodologies and may be requested to attend an on-site meeting at one of the USDA office locations (in Ft. Collins, CO, or Washington DC).

The Contractor PM will be a direct liaison to the Contracting Officer's Representative (COR), the Government Program Manager or Section Chief, Government Tactical Project Manager(s), Technical Points of Contact (TPOC), Government Business Owners, and/or Government Product Owner(s) as necessary. The Contractor PM is responsible for the supervision and management of the Contractor's personnel, technical assistance, and interface.

The Contractor PM must have relevant experience managing complex IT projects, managing a large IT portfolio of projects, and implementing SAFe® development methodology.

Desired skills and experience for the Contractor Program Manager include:

- Experience in technical leadership,
- Ability to rapidly prioritize competing requirements,
- Ability to understand and simplify customer requirements,
- Ability to communicate end user feedback to technical and design leads,
- Strong communication skills,
- Proven knowledge of industry standards.

The Contractor PM must have a full understanding of the technical approach discussed in the Contractor's Proposal and delivered by the Contractor after award.

3.6.2 Release Train Engineer (RTE)

As a part of the critical path to success, the Value Stream ART Engineer (RTE) is required key personnel. The Government expects that the RTE be dedicated for the duration of the period of performance.

Per the Scaled Agile Framework, the RTE must be a servant leader and coach for the Value Stream ART. The RTE's major responsibilities are to facilitate the ART events and processes and assist the teams in delivering value. At a minimum, the RTE will facilitate PI planning, manage risks and dependencies, escalate and track impediments,

coach team leaders and scrum masters, facilitate synchronization events, and communicate with all other RTEs within the Conservation Solution.

3.6.3 Contractor Solution Manager

As a part of the critical path to success, the Value Stream ART Solution Manager is required key personnel. The Government expects that the Solution Manager be dedicated for the duration of the period of performance.

The Solution Manager will participate as a member of the Solution Train team. Solution Management is responsible for defining and supporting the building of desirable, feasible, viable, and sustainable large-scale business solutions that meet customer needs.

The Solution ART includes the following roles:

1. Solution Train Engineer
2. Solution Architect
3. SAFe ® Coach
4. Release Manager
5. Data Architect
6. Value Stream ART Solution Manager

The Government provides the first five roles of the Solution Train team via a separate Solution ART contract. The Contractor for each Value Stream ART provides a Solution Manager to represent customer needs, understand the solution context that their Value Stream ART provides, and work collaboratively to develop the Solution Vision.

Solution Managers play a critical role in solution train events including Pre-PI and Post-PI planning, Solution and System Demos, Solution Train Sync, and the Inspect and Adapt (I&A) Workshops. This role is a customization of the Solution Manager role defined by SAFe®.

The Solution Managers will be members of the Solution Train but will very much work to represent their Value Stream ART at the Solution level. Solution Managers will work collaboratively to perform the following responsibilities:

- Collaborate with necessary Value Stream ART stakeholders to steward continued release of valuable business outcomes resulting in the progression of developing better quality software.
- Facilitate the application of reporting/tracking standards that will be used across the ARTs consistently. Standards including but not limited to the consistent use of defect status and defect tracking, and workflows that assist in assigning user stories to releases consistently. The Solution Manager will help develop standards while considering the impacts to the ARTs and overall usage of these standards to improve the Solution.
- Work collaboratively with other Solution Train team members to understand the broader context and to recognize/address cross-train dependencies and risks. Crosstrain dependencies need to be tracked and managed at the Solution Train level. Solution managers will represent their ART in creating action plans for addressing cross-train dependencies and facilitating discussions/providing solutions to address the dependencies.
- Develop/Improve the Knowledge Transfer (KT) process. ART Solution Managers will represent their ART and participate in Knowledge Transfer activities to assess areas of improvement and maintain the

integrity of the process. Continue to enhance the KT process including but not limited to defining the definition of done and defining conditions that support a successful KT process.

- Work collaboratively with Release Manager, DSO, PSO, Security and GPMs to assist in deployment activities with activities including but not limited to process improvement and enhancing communication particularly when it involves cross-train dependencies/regression.
- Assist in developing Solution Backlogs that result in delivering better quality software to the customer.
- Help to facilitate the SAFe® set-based design (SBD) practice across the solution backlog.
- Continually refine the solution backlog capabilities and solution epics working with both government and development product management teams.
- Explore multiple options to delivering value and remain flexible.
- Coordinate refinement meetings as needed and utilize the Weighted Shortest Job First (WSJF) prioritization model to prioritize the solution backlog.
- Define and maintain the solution intent collaborating with other solution managers.
- Adjust solution intent based on feedback during PI execution.
- Assist with coordination for software efforts that are train-aligned or related to a train but not on a train.
- Manage functional requirements; assure alignment with both government and development product management and define solution intent.
- Collaborate with Solution Architect(s) to design the solution, enable technical probability, and support the architecture runway.
- Work with STE, RTE, independent verification group and Value Management Office (VMO) to maintain metrics and radiators to show transparency, alignment, execution, and quality.
- Manage solution level risks using Jira, assign ROAM (resolved, owned, accepted, mitigated) categories during PI planning and burndown during PI execution.
- Define, facilitate, educate, and align PI (PI) solution demos with ART PI system demos working with both government and development product management teams.
- Attend and contribute to all Solution Train ceremonies.
- Other duties as assigned related to improving efficiencies and processes associated with the solution.

3.6.4 Contractor Product Manager

As a part of the critical path to success, the Value Stream ART Product Manager is required key personnel. The Government expects that the Train Product Manager be dedicated for the duration of the period of performance.

The Product Manager shall provide and ensure cross-train product coordination with other Value Stream ARTs, other contractor teams that may operate outside of any single ART, and cross-team coordination within each ART. The Product Manager supports the Product Owner and shall ensure epics and features that cross teams are prioritized correctly to effectively produce software releases in a timely manner and develop product roadmaps or portfolio epic roadmaps that maximize product integration across the ART and reduce duplication of work in teams. The Product Manager must effectively collaborate and support end to end development to ensure

delivery as planned. The Product Manager shall communicate and evaluate cross-train work in conjunction with the Government Business Owner and Government Product Owners to maximize collaborative work while balancing dedication to project scope, schedule, and budget.

3.6.5 Information on Historical Skillsets and Experience

Based on historical performance, the Government identified the following skillsets and experience as beneficial. This content is informational only. The Contractor shall determine the appropriate skillsets and experience to meet PWs performance standards. (bullet list will be tailored by value stream)

- Java
- C#/.Net
- LoadRunner
- ESRI JS API
- Geospatial applications and ArcGIS
- PostgreSQL and PostGIS development
- Drupal
- Microsoft SQL
- Python programming and R programming languages
- Machine Learning
- Business analysis
- User centered design
- Product management
- Agile software development
- Systems integration
- Unit, functional (include UI and API), integration, end-to-end, 508 conformance, and performance testing
- DevOps
- Scrum, Release Train, and Solution Train Leadership with SAFe® certification when operating in a train.
- Front End Engineers with experience in the following areas:
- Scrum Development
- JavaScript
- Customer Service Skills
- User Experience Testing
- Back End Engineers with experience in the following areas:
- Cloud deployment in Infrastructure as a Service (IaaS) or Platform as a Service (PaaS) environments.

- Full Stack Engineers with a combination of the experience areas from both Front and Back- end Engineers.
- Security Engineers with experience in the following areas:
- SSO (Single Sign On) mechanisms such as SAML and OAuth2.0
- Performing security audits, risk analysis and threat modeling
- Pega

4 General Requirements

4.1 Deliverable Acceptance and Inspection

Code deliverables will be submitted via a Git or SVN repository. Per PWS instructions, a copy of any document deliverables may be required to be submitted to the COR, GPM, TPOC, Product Owner, and/or Product Manager(s) and uploaded to a location determined by the government.

Within 5 business days of each iteration's completed delivery, the Government will inspect, review, and accept all periodic reports and task deliverables, as applicable. If rework is needed, a revised timeline will be set forth with a similarly constrained review upon resubmission.

Supporting IT Application Development, at the end of each iteration or sprint, the Contractor team(s) shall be required to demonstrate to the government product owners the work performed within the iteration/sprint. Government Product Owners are responsible for feature and user story acceptance. In the event the government product owner desires a change to the work performed and demonstrated, the change shall be managed by adding the changes required to the Program Backlog and prioritized accordingly for the next iteration or sprint. It is expected that the Contractor shall recognize this as a change request and not take this on as a "defect". It should also be expected that the government will assess the change versus defect decision and will hold to proper process based on the final adjudication, as decided by the Government. The final goal in agility is to get quality product to the product owner in the way it is needed, while following the process.

The COR may work with other Government personnel to monitor technical progress (e.g. Government PM or Technical Point of Contact). The Contractor shall work with other Government personnel, as designated by the COR, in review of specified requests and implementation of the specified task assignment request. Any actions resulting from such interactions that affect the contract or scope of work, or administrative issues, including work schedules and resources, must be documented, and reported to the COR and the Contracting Officer (CO), as appropriate, for approval before being implemented by the Contractor. The Contractor must bring problems or potential problems affecting performance to the attention of the COR as soon as possible. Verbal reports must be followed up with written reports, when directed by the COR, within twenty-four (24) hours. The Contractor shall preferably find opportunities for the Government personnel (COR, TPOC) to attend demos or other "live events" where functionality may be proved out enabling approval of written planned activities. The goal is to reduce duplicative reporting and administrative burden on both the Government and Contractor. Both parties shall be mindful of how this accomplishes stewardship and documentation requirements for example, developing "performance acceptance templates" which will support invoicing.

Only the CO may act affecting the contractual relationship between the Government and the Contractor, including interpreting, or changing the terms and conditions of the contract. The Contractor must not contact

nor take direction from unauthorized FPAC employees, under any circumstances. The Contractor must direct all written and/or oral communications, throughout the project life cycle, to the CO and the COR.

4.2 Period of Performance

The period of performance of this PWS is one (1) 12-month base period, followed by four (4) 12-month option periods. Each contract period includes four program increments.

Planned period of performance:

Contract Period	Dates	Program Increments
Base Period	4/9/2025 – 4/8/2026	30 – 33
Option Period 1	4/9/2026 – 4/8/2027	34 – 37
Option Period 2	4/9/2027 – 4/8/2028	38 – 41
Option Period 3	4/9/2028 – 4/8/2029	42 – 45
Option Period 4	4/9/2029 – 4/8/2030	45 – 49

4.3 Place of Performance

The Contractor primarily will work off site. The Government is not requiring onsite support at this time, but limited on-site presence may be required in the future. The Contractor PM may be requested to attend on-site meetings at one of the USDA office locations (in Ft. Collins, CO, or Washington DC). Any future requirements for on-site presence will be added via a contract modification with a price adjustment if needed.

4.4 Hours of Work

The Government's normal duty hours are 6 a.m. – 6 p.m. local time and core work hours are 9:00 a.m. – 3:00 p.m. local time. Work performed at Government facilities should be accomplished during normal duty hours. If work must be performed at Government facilities outside normal duty hours, the Contractor must alert the COR. Contractor personnel will not report to Government facilities to work nor remain at the work locations any time the Government is unexpectedly required to close their offices. The Contractor will not be compensated for these Government closures. The Contractor is responsible for all notification of their contractor staff during times of closure.

A normal workweek is Monday through Friday, except Federal Holidays. Exceptions may apply, for example, Contractors supporting production support operations shall perform work outside these regular hours of operations in support of planned and unplanned maintenance and operations activities.

4.5 Holidays and Administrative Leave

The Contractor is hereby advised that Government personnel observe the following holidays: New Year's Day, Martin Luther King's Birthday, President's Day, Memorial Day, Independence Day, Juneteenth, Labor Day, Columbus Day, Veteran's Day, Thanksgiving Day, and Christmas. In addition to the days designated as holidays, the Government may observe any other days designated by Federal Statute, any other days designated by

Executive Order, and any other days designated by the President's Proclamation. This includes Inauguration Day (Washington, D.C. metropolitan area only). Observance of such days by Government personnel must not be a reason for an additional period of performance, or entitlement of compensation.

When the agency grants administrative leave to its employees, on-site assigned Contractor personnel may be dismissed by the Contractor. The Contractor agrees to continue to provide sufficient personnel to perform tasks already in operation or scheduled, and must be guided by the instructions issued by the COR. The Government will not pay for the labor hours during the leave granted to non-working contract personnel because of inclement weather, potentially hazardous conditions, explosions, and other special circumstances.

4.6 Continuity of Operations (COOP)/Disaster Recovery Temporary Relocation

The National Security Presidential Directive/NSPD-51/Homeland Security Presidential Directive/ HSPD-20, National Continuity Policy, requires Federal departments and agencies to maintain a comprehensive and effective continuity capability, including a Continuity of Operations (COOP) program. The COOP program, which also includes pandemic preparedness, ensures the continuation of essential functions under emergency situations.

An emergency may require personnel to temporarily relocate to a pre-designated, alternate work site or telework to ensure continuity of essential functions. A contract position may support the FPAC COOP plan, and the Contractor may be required to report for work to assist the federal staff in supporting critical business functions following a formal disaster declaration. Contractor employees, under this scenario, are required to deploy to the alternate work site within 12 hours of COOP Plan activation for the support of Government identified essential functions. The deployment to the alternative work site may last for up to 30 days. Travel and per diem expenses, if required, will be reimbursed in accordance with the Federal Travel Regulation (FTR).

The Government will also engage in “PLANNED” Disaster Recovery Exercises throughout a given Fiscal Year. As these exercises are typically planned well in advance, FPAC may require Contractor employees’ participation in these exercises after appropriately coordinated advance notice. There may also be the limited possibility of an “UN-PLANNED” Disaster Recovery Exercise. Unplanned exercises are typically conducted during business hours and Government may require Contractor employees’ participation after immediate notice. Travel is not expected to be required during Disaster Recovery exercises/testing.

4.7 Work Locations Requiring Non-Local Travel

The Contractor may be required to support non-commuter travel in support of this task order, as required by the Government. The COR (as delegated by the CO) has sole authority to approve non-local travel requests necessary to support contract performance. Not later than five (5) business days prior to the Contractor’s estimated date of departure, the Contractor must submit a travel request to the COR, to include travel justification, the proposed itinerary, and cost estimates for such travel. Reimbursement of travel costs shall be in accordance with FAR subsection 31.205-46. The Contractor must be responsible for all travel arrangements including airline, hotel, and rental car reservations. The Contractor must make every commercially reasonable effort to schedule travel far enough in advance to take advantage of reduced airfares. Expenses shall be forecast, tracked, and invoiced by event, i.e., PI planning or specific workshops.

4.8 Government Furnished Equipment

GFE is property in the possession of, or directly acquired by, the Government and subsequently furnished to the contractor for performance of a contract. (FAR Part 45)

The Government will provide laptops, docking stations, and peripherals without cost. In addition, the Government will provide access to software licenses and environments required to perform work under this PWS. The Government furnished property and services provided as part of this contract must be used only by the Contractor only to perform under the terms of this contract. No expectation of personal privacy or ownership using any USDA electronic information or communication equipment must be expected. All property at Government work sites, except for Contractor personal items will be assumed to be Government property unless an inventory of Contractor property is submitted and approved by the CO/COR. Contractor personal items do not include computers, external drives, software, printers, and/or other office equipment (e.g., chairs, desks, file cabinets). The Contractor must maintain an accurate inventory of Government furnished property.

Government Furnished Equipment (GFE) may only be taken on international travel if the travel is contractually authorized and has prior approval in writing by all required federal parties (e.g., contracting office, contracting officer's representative (COR), Federal project manager (PM), FPAC Assistant Chief Information Security Officer, etc.). On the rare occasion GFE is approved for use during international travel, the Contractor(s) must follow all FPAC Policies and Standard Operating Procedures (SOP).

In the context of GFE use, international travel is defined as travel outside the fifty (50) United States (U.S.) and District of Columbia (DC). Travel to U.S. territories (e.g., Puerto Rico, U.S. Virgin Islands, Guam, etc.) is considered international travel.

FPAC does not authorize GFE for personal international travel (e.g., vacation, family emergency, etc.). FPAC does not authorize GFE for non-governmental business international travel (e.g., business not in direct performance of the contract for which the GFE is provided).

5 Additional Technical Standards

5.1 Cybersecurity/Supply Change Risk Management

5.1.1 Country of Origin

Country of Origin (COO) represents the country or countries of manufacture, production, design, or brand origin. The expectation is: (1) the cargo is what it purports to be and in the quantity stated; (2)the cargo was in the continuous possession or control by the carrier who took charge of the cargo from the time it was loaded in the container at origin until the time it is delivered at final destination; and (3) there is evidence of the identify of each person or entity who had access to it during its movement and that the cargo remained in the same condition from the moment it was sealed in the container for transfer to the carrier who controlled possession until the moment that carrier released the cargo into the receipted custody of another.

Country of Origin guidelines are as follows:

a. USDA will not use any product or its components (including hardware, software, and firmware) that are on the *Department of Commerce Entity List*. This includes countries where the development, manufacturing, maintenance, and service for the product are provided.

b. Contractor or Sub-Contractor shall identify the country (or countries) of origin of the procured product and its components (including hardware, software, and firmware).

c. Contractor or Sub-Contractor will identify the countries where the development, manufacturing, maintenance, and service for the product are provided.

d. Contractor or Sub-Contractor will notify USDA of changes in the list of countries where product maintenance or other services are provided in support of the procured product. This notification shall occur # days prior to initiating a change in the list of countries.

e. Contractor or Sub-Contractor shall ensure that all-source threat and vulnerability information includes any available foreign ownership and control (FOCI) data. This data should be reviewed periodically as mergers and acquisitions, if affecting a supplier, may impact both threat and vulnerability information and therefore SCRM.

f. Contractor or Sub-Contractor shall use trusted channels to ship procured products, such as U.S. registered mail.

g. Contractor or Sub-Contractor shall demonstrate a capability for detecting unauthorized access throughout the delivery processes.

h. Contractor or Sub-Contractor shall demonstrate chain-of-custody documentation for procured products as determined by USDA in its sole discretion and require tamper-evident packaging for the delivery of this product.

5.1.2 Personnel and Certification Requirements

5.1.2.1 Personnel

5.1.2.1.1 Background Check

As part of the Homeland Security Presidential Directive (HSPD) 12, *Homeland Security Presidential Directive 12: Policy for a Common Identification Standard for Federal Employees and Contractors*, each Contractor or Sub-Contractor must provide identity documentation, as set forth in the Form (I-9), and the validity of the documentation is certified by at least three other checks incorporated into the ID-Proofing process.

a. Contractor or Sub-Contractor shall comply with the personal identity verification (PIV)policies and procedures established by the Department of Agriculture (USDA) Directives4620-002 series - *Common Identification Standard for U.S. Department of Agriculture Employees and Contractors*.

b. Should the results of the PIV process require the exclusion of a Contractor or Sub-Contractor's employee; the Contracting Officer Representative (COR) shall notify the Contracting Officer (CO) in writing.

c. The Contractor or Sub-Contractor must appoint a representative to manage compliance with the PIV policies established by the USDA Directives 4620-002 series and to maintain a list of employees eligible for a USDA LincPass required for performance of the work.

d. The responsibility of maintaining a sufficient workforce remains with the Contractor or Sub-Contractor. Employees may be barred by the Government from performance of work should they be found ineligible or to have lost eligibility for an USDA LincPass. Failure to maintain a sufficient workforce of employees eligible for an USDA LincPass may be grounds for termination of the contract.

e. The Contractor or Sub-Contractor shall insert this clause in all subcontracts when the Contractor or Sub-Contractor is required to have routine physical access to a federally controlled facility and/or routine access to a federally controlled information system.

f. The PIV Sponsor for this contract is a designated program point of contact, which in most cases is the COR, unless otherwise specified in this contract.

In addition to meeting the requirements of HSPD-12 for PIV (I and II process), all Contractor or Sub-Contractors requiring routine physical access for Federally-controlled facilities and/or routine access to Federally-controlled information systems must have been successfully identity proofed and successfully adjudicated National Agency Check with Written Inquiries (NACI) or Office of Personnel Management (OPM)/National Security (NS) community background investigation to serve on a USDA contract. Contract personnel must have a minimum of a NACI or higher level of background investigation depending on the Position Sensitivity Designation (PSD).

5.1.2.1.2 Position Sensitivity Designations (PSDs)

All positions within USDA are assigned Position Sensitivity Designations (PSDs) based upon the risk/damage an unauthorized disclosure would cause to the Agency and/or National Security. This includes positions occupied by Contractors or Sub-Contractors. The Contracting Officer (CO) and/or Contracting Officer Representative (COR) will identify and assign a Position Sensitivity Designation Code to each position that will be occupied by a Contractor or Sub-Contractor in the performance of the contract. The CO/COR will advise the Contractor or Sub-Contractor of the assigned designation and investigative requirements at the offset of contract talks. The minimum Public Sector Information (PSI) for a Contractor or Sub-Contractor is National Agency Check with Law Enforcement and Credit Check (NACLC). However, based upon the assigned sensitivity code, the minimum level PSI may not meet the requirements, and a higher level of investigation and/or Security Clearance may be required. The Contracting Officer Representative (COR) will submit all investigative and/or clearance data to the Physical Security Team (PST) five (5) days prior to the Contractor or Sub-Contractor's first day of work. The PSDs are separated into two categories, Public Trust Positions (Risk) and National Security Positions.

a. Public Trust Positions: These positions are identified as Low Risk, Moderate Risk, and High Risk. They are numerically identified as 1, 5, and 6, respectively. Each of these designations requires a different PSI and a favorable Suitability Determination. Public Trust Positions do not require Personnel Security Clearances.

b. National Security Positions: These positions are identified as Non-Critical Sensitive, Critical Sensitive and Special Sensitive. They are numerically identified as 2, 3 and 4, respectively. Each of these designations requires a different PSI and a favorable Security Determination. National Security Positions require a Personnel Security Clearance equal to or higher than the level of Access required performing the duties. The level of Clearance is requested at the time the PSI is submitted.

For Position Sensitivity Designation (PSD) for Contract Employees, the Contractor or Sub-Contractor will submit proof of their contract employee's investigative and/or clearance data to the COR five (5) days prior to the Contractor or Sub-Contractor's first day of work.

Only appropriately cleared Contractors or Sub-Contractors will be utilized in the performance of this Contract. The Physical Security Team will review all investigated and clearance data submitted by the Contractor or Sub-Contractor on behalf of their employees and determine its validity. Should any contract employee be removed for security or suitability reasons, it is incumbent on the Company to provide a replacement that meets or exceeds all PSI and/or Clearance requirements. Any failure of the Contractor or Sub-Contractor to comply with the Personnel Security requirements may result in the termination of the Contractor or Sub-Contractor and/or Contract for default/cause.

Contractor or Sub-Contractor ID credentials will be issued after successful identity proofing of the Contractor or Sub-Contractor employee applicant and upon verification of a successfully adjudicated NACI or OPM/NS BI.

For more information about HSPD-12, see https://hspd12.usda.gov/.

5.1.2.1.3 Contractor or Sub-Contractor System Access

The Contracting Officer or Contracting Officer's Representative will work with the project manager and/or supervisor to determine the appropriate security access required by the Contractor. USDA will ensure access is commensurable with the functions to be performed by utilizing the RBAC (Role-Based Access Concept).

5.1.2.1.4 Non-Disclosure Agreement

All Contractor and Sub-Contractor cybersecurity personnel must submit a Non-Disclosure Agreement, "Employee/Contractor or Sub-Contractor Non-Disclosure Agreement" form, prior to the commencement of any cybersecurity work on the contract. Further, Contractor or Sub-Contractor and Contractor or Sub-Contractor personnel must submit a non-disclosure agreement whenever replacement personnel are proposed. Any information provided by the Contractor or Sub-Contractor or Contractor or Sub-Contractor in the performance of this contract or obtained by the government is only to be used in the performance of this contract.

5.1.2.1.5 Contractor or Sub-Contractor Termination / Resignation

Upon termination, resignation or other event leading to a contract employee leaving duty under this contract, the contract employee is responsible for returning all Government identification, vehicle passes, other Government property or anything considered Government Furnished issued to the employee. Such material shall be returned to the Contracting Officer's Representative. Failure on the part of the employee to return such property may result in the Contractor or Sub-Contractor's liability for all costs associated with correcting the resultant breech in building security. Refer to FAR for specific details.

5.1.3 Cybersecurity Certification and Training

5.1.3.1 Computing Environment (CE) Certification

The computing environment involves the collection of computer machinery, data storage devices, workstations, software applications, and networks that support the processing and exchange of electronic information demanded by the software solution. The various types of CE include Personal, Time Sharing, Client Server, Distributed, Cloud and Cluster. Therefore, Contractor or Sub-Contractor shall have the required certification for the computing environment.

5.1.3.2 Cybersecurity Maturity Model Certification (CMMC)

USDA SCRM Strategy applies to systems operated by USDA and entities not under the jurisdiction of the USDA Secretary that are employed or contracted to process, transmit, or store USDA information through services such as (but not limited to), platform as a service (PaaS), infrastructure as a service (IaaS), and software as a service (SaaS.). In accordance with USDA DR 3540-003, The Contracting Officer Representative/Program Manager will certify that Contractor or Sub-Contractor has the appropriate DOD Cybersecurity Maturity Model Certification (CMMC) level as prescribed by USDA and outlined below.

5.1.3.3 Information Security Awareness Training

The Contracting Officer Representative/Program Manager will certify that Contractor or Sub-Contractor personnel have completed the required Information Security Awareness and Rules of Behavior Training prior to submission of a Security Access Requests.

5.1.4 Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM) Software Development Lifecycle (SDLC)

Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM) Software Development Lifecyle (SDLC) is implemented as part of overall risk management activities, such as those described in NIST SP 800-39, *Managing Information Security Risk*. Activities should involve identifying and assessing applicable risks, determining appropriate mitigating actions, developing an ICT SCRM Plan to document selected mitigating actions, and monitoring performance against that Plan.

Contractor or Sub-Contractor shall ensure the latest publication of NIST SP 800-161 - *Supply Chain Risk Management Practices for Federal Information Systems and Organizations* and NIST SP 800-37 - *Risk Management Framework for Information Systems and Organizations* are incorporated into their ICT SCRM SDLC process.

Consistent with the latest publication of NIST SP 800-161 and NIST SP 800-37, the acquisition community at the USDA and agencies will adopt an ICT SCRM SDLC approach to managing risk to information systems. The USDA, agencies, and personnel will integrate SCRM processes, activities and tasks throughout the life cycle of agency systems, components and services.

5.1.4.1 Continuous Diagnostic and Mitigation (CDM) Approved Products List (APL) Supply Chain Risk Management Plan

The Continuous Diagnostics and Mitigation (CDM) Approved Products List (APL) Product Submission Instructions reference the requirement to submit a Supply Chain Risk Management Plan (SCRM) as part of that activity. The CDM APL SCRM Plan is in support of the National Institute of Standards (NIST) and the latest publication of NIST Special Publication (SP) 800-53 “SA-12” supply chain control. Contractor or Sub-Contractor is responsible for providing the CDM APL SCRM Plan. The purpose of this document is to provide background information on the SCRM requirement and outline the instructions an offeror is to follow in completing and submitting the CDM APL SCRM Plan. The CDM APL SCRM Plan consists of (1) the completed questionnaires and (2) additional information the offeror wishes to provide. APL submission packages that do not include completed CDM-APL-SCRM questionnaires will fail conformance. Additional information can be submitted; APL packages will not fail conformance for the lack of providing SCRM information beyond the questionnaires for CDM-APL-SCRM.

The objective of CDM SCRM Plan is to provide information to Agencies and ordering activities about how the offeror identifies, assesses, and mitigates supply chain risks to facilitate better informed decision-making by Agencies and ordering activities. The CDM SCRM Plan is intended to provide visibility into, and improve the buyer’s understanding of, how the Offeror’s proposed products are developed, integrated and deployed; as well as the processes, procedures, and practices used to assure the integrity, security, resilience, and quality of those products.

The Contractor shall include a CDM SCRM Plan with its proposal that addresses counterfeit and illegally modified products. The CDM SCRM plan shall describe the contractor’s approach to SCRM and demonstrate how the contractor’s approach will reduce and mitigate supply chain risks. For additional details on GSA’s internal guidance on supply chain risk management, see subpart GSAM 504.70.

The Contractor shall provide a CDM SCRM plan to manage supply chain risk throughout each of the five (5) supply chain phases specified in its proposal: 1) design and engineering, 2) manufacturing and assembly, 3) distribution and warehousing, 4) operations and support, and 5) disposal and return. In addition to the components and processes for which the contractor is directly responsible, and as feasible, the contractor shall

identify “specified supporting infrastructure beyond the system boundary” and where appropriate, include such infrastructure in its SCRM Plan.

The CDM SCRM Plan shall address at a minimum, but not be limited to, the following:

1) How the contractor ensures that requirements for genuine Information Technology Tools (ITT) are imposed upon its direct suppliers, whether the direct supplier is a systems integrator, reseller or OEM. The requirements for assurance and supporting evidence must include:
    a) The contractor performs reasonable steps to ensure its SCRM Plan is performed for ITT in its delivered and installed configuration.
    b) Equipment resellers from whom the contractor purchases ITT have valid licenses for OEM equipment and software.
    c) The ITT OEM exercises strict quality control to ensure that counterfeit or illegally modified hardware or software components are not incorporated into the OEM product; and
    d) The contractor ensures traceability of assurance and evidence of genuineness of ITT back to the licensed product and component OEMs.
2) The contractor’s use of system security engineering processes in specifying and designing a system that is protected against external threats and against hardware and software vulnerabilities.
3) The contractor’s strategy for implementing SCRM security requirements throughout the life of the contract. The SCRM plan shall address the security controls described in the latest publication of NIST SP 800-53. Implementation of the controls shall be tailored in scope to the effort and the specific information.
4) The criticality analysis (CA) process used by the contractor to determine Mission Critical Functions, and the protection techniques (countermeasures and sub-countermeasures) used to achieve system protection and mission effectiveness. The CA shall describe the contractor’s supply chain for all critical hardware and software components (and material included in products), key suppliers, and include proof of company ownership and location (on-shore or off-shore) for key suppliers and component manufacturers.
5) How the contractor will ensure that products and components are not repaired and shipped as new products and components are provided to the government.
6) How the contractor will ensure that supply channels are monitored for counterfeit products throughout the product life cycle to include maintenance and repair.
7) How the contractor’s physical and logical delivery mechanisms will protect against unauthorized access, exposure of system components, information misuse, unauthorized modification, or redirection.
8) How the contractor’s operational processes (during maintenance, upgrade, patching, element replacement, or other sustainment activities) and disposal processes will limit opportunities for knowledge exposure, data release, or system compromise.
9) Which of the following identifies the relationship between the contractor and the manufacturer: 1) OEM, 2) authorized reseller, 3) authorized partner/distributor, or 4) unknown/unidentified source.
10) How the contractor will ensure independent verification and validation of assurances, and provide supporting evidence as required.

NIST SP 800-161 identifies supply chain risk management (SCRM) best practices. The offeror shall update its SCRM Plan to include any future changes to the NIST SCRM Guidelines and all such modifications to the Plan shall be made at no cost to the government.

5.1.4.2 SCRM Plan Submittal and Review

The plan shall be submitted with the contractor's proposal. Updates shall be submitted on an annual basis to the CO and COR. All information included will be treated as Controlled Unclassified Information (CUI) pursuant to Executive Order 13556, shared only with government agencies, and used solely for the purposes of mission-essential risk management. All reviews shall be completed within a 45-day period.

5.1.4.3 Manufacturing (Original Equipment Manufacturer (OEM)

Contractor or Sub-Contractor developers shall perform industry best practices associated with security testing and evaluation consistent with the latest publication of Special Publication 800-115 - *Technical Guide to Information Security Testing and Assessment*. This includes, but is not limited to, the following:

- Implement a repeatable and documented assessment methodology,
- Analyze findings, and develop risk mitigation techniques to address weaknesses,
- Provide consistency and structure to security testing, which can minimize testing risks, and
- Address resource constraints associated with security assessments.

5.1.4.3.1 Counterfeit Parts/Replacement Parts

A product is genuine if it is not counterfeited, imitated, tampered or adulterated and is not gray market, remanufactured, or refurbished. Contractor or Sub-Contractor shall report all suspected counterfeit material/items to the Government through the Government Industry Data Exchange Program (GIDEP) database and to the program office via e-mail to the Contracting Officer, Program Manager, and COR within # working days of discovery. The Contractor or Sub-Contractor shall prominently label all suspected counterfeit material/items and physically separate from all other supplies and shall not return or dispose suspected or confirmed counterfeit material/items to the supplier but hold such items for Government analysis and investigation. The Contractor or Sub-Contractor shall aid the Government investigation including providing all documents associated with the purchase, shipping, and other relevant data on the counterfeit materials/items. The Government will provide final disposition instructions for confirmed counterfeit material/items to include turnover to the Government.

5.1.4.4 End of Life/Support Products

Any product within 18 months of End of Life/End of Support will not be procured by USDA.

5.1.4.4.1 Product Integrity [GSA SECTION 846 – COUNTERFEIT ITEMS]

5.1.4.4.1.1 Hardware, Software, and Patch Integrity and Authenticity:

If Contractor or Sub-Contractor provides software or patches to USDA, Contractor or Sub-Contractor shall publish or provide a hash conforming to the Federal Information Processing Standard (FIPS) Security Requirements for Cryptographic Modules (FIPS 140-2) or similar standard information on the software and patches to enable USDA to use the hash value as a checksum to independently verify the integrity of the software and patches and avoid downloading the software or patches from Contractor or Sub-Contractor's website that has been surreptitiously infected with a virus or otherwise corrupted without the knowledge of Contractor or Sub-Contractor.

a. Contractor or Sub-Contractor is responsible for providing software that is free of vulnerabilities by validating that those Common Vulnerability and Exposures (CVE), common weakness enumeration (CWE).

b. Open Web Application Security Project (OWASP) items that are most dangerous to the mission are absent from the software and that the software operates at the least privilege required to complete its task; and

c. Contractor or Sub-Contractor shall establish, document, and implement risk management practices for supply chain delivery of hardware, software (including patches), and firmware provided under this Agreement.

5.1.4.4.1.2 Digital Delivery

Contractor or Sub-Contractor shall specify how digital delivery for procured products (*e.g.*, software, applications, and data) including patches will be validated and monitored to ensure the digital delivery remains as specified. If USDA deems that it is warranted, Contractor or Sub-Contractor shall apply encryption to protect procured products throughout the delivery process.

5.1.4.4.1.3 Firmware

a. Prior to the delivery of any products and services to USDA or any connection of electronic devices, assets or equipment to USDA's electronic equipment, Contractor or Sub-Contractor shall provide documentation regarding its patch management and vulnerability management and continuous monitoring (including third-party hardware, software, and firmware) for products, services, and any electronic device, asset, or equipment required to be connected to the assets of USDA during the provision of products and services under this Agreement. This documentation shall include information regarding:

- Resources and technical capabilities to sustain this program and process such as Contractor or Sub-Contractor's method or recommendation for how the integrity of a patch is validated by USDA,
- Contractor or Sub-Contractor procedures to Check Software and the patches for authenticity and integrity of the products with integrity verification tools, to detect unauthorized changes to software, information system and the supply chain. An example of a validation procedure may be the use of digital signature by an OEM to prove that the software delivered is from its originating source. When digital signatures are used for this purpose, the organization should ensure, when receiving such software, that the signed upgrade/download was not altered,
- USDA will ensure that code authentication mechanisms such as digital signature, certificate is recognized and approved,
- Implement the use of cryptographic mechanisms, to authenticate software, hardware, information systems within the supply chain infrastructure,
- Contractor or Sub-Contractor's approach and capability to remediate newly reported zero-day vulnerabilities, and
- Contractor or Sub-Contractor shall ensure all developers are trained and held accountable for development of secure code.

b. Unless otherwise approved by the USDA in writing, current or supported version of Contractor or Sub-Contractor products and services shall not require the use of out-of-date, unsupported, or end-of-life version of third-party components (*e.g.*, Java, Flash, Web browser, etc.).

c. Contractor or Sub-Contractor shall verify and provide documentation that procured products (including third-party hardware, software, firmware, and services) have appropriate updates and patches installed prior to delivery to USDA.

d. In providing the products and services described in this Agreement, Contractor or Sub-Contractor shall provide appropriate software and firmware updates to remediate newly discovered vulnerabilities or weaknesses within 30 days. Updates to remediate critical vulnerabilities shall be provided within a shorter period than other updates, within *14 days*. If updates cannot be made available by Contractor or Sub-Contractor within these time periods, Contractor or Sub-Contractor shall provide mitigations within a negotiated period.

e. When third-party hardware, software (including open-source software), and firmware is provided by Contractor or Sub-Contractor to USDA, Contractor or Sub-Contractor shall provide appropriate hardware, software, and firmware updates to remediate newly discovered vulnerabilities or weaknesses within [a negotiated period]. Updates to remediate critical vulnerabilities shall be provided within a shorter period than other updates, within *14 days*. If these third-party updates cannot be made available by Contractor or Sub-Contractor within these time periods, Contractor or Sub-Contractor shall provide mitigations within a negotiated period.

5.1.4.4.2 Viruses and Malware

Contractor or Sub-Contractor will use reasonable efforts to investigate whether computer viruses or malware is present in any software or patches before providing such software or patches to USDA.

a. Contractor or Sub-Contractor warrants that it has no knowledge of any computer viruses or malware coded or introduced into any software or patches, and Contractor or Sub-Contractor will not insert any code which would have the effect of disabling or otherwise shutting down all or a portion of such software or damaging information or functionality.

b. When installed files, scripts, firmware, or other Contractor or Sub-Contractor deliverer software solutions are flagged as malicious, infected, or suspicious by an anti-virus vendor through open-source solutions, Contractor or Sub-Contractor must provide technical proof as to why the “false positive” hit has taken place to ensure their code’s supply chain has not been compromised.

c. If a virus or other malware is found to have been coded or otherwise introduced because of Contractor or Sub-Contractor’s breach of its obligations under this Agreement, Contractor or Sub-Contractor shall immediately and at its own cost:

    - Take all necessary remedial action and aid USDA to eliminate the virus or other malware throughout USDA’s information networks, computer systems, and information systems, regardless of whether such systems or networks are operated by or on behalf of USDA; and
    - If the virus or other malware causes a loss of operational efficiency or any loss of data (A) where Contractor or Sub-Contractor is obligated under this Agreement to back up such data, take all steps necessary and provide all assistance required by USDA and its affiliates, and (B) where Contractor or Sub-Contractor is not obligated under this Agreement to back up such data, use commercially reasonable efforts, in each case to mitigate the loss of or damage to such data and to restore the efficiency of such data.

5.1.4.5 Transport/Shipping

5.1.4.5.1 Chain of Custody

Chain of Custody apply throughout the ICT SCRM SDLC phases; therefore, refer to Section 5.1.5.1 – Chain of Custody.

5.1.4.5.2 Anti-Tamper Testing/Inspection

Tamper Resistance and Detection apply throughout the ICT SCRM SDLC phases; therefore, refer to Section 5.1.5.2 – Anti-Tamper and Detection.

5.1.4.6 Pre-Deployment

5.1.4.6.1 Chain of Custody

Chain of Custody apply throughout the ICT SCRM SDLC phases; therefore, refer to Section 5.1.5.1 – Chain of Custody.

5.1.4.6.2 Anti-Tamper Testing/Inspection

Tamper Resistance and Detection apply throughout the ICT SCRM SDLC phases; therefore, refer to Section 5.1.5.2 – Anti-Tamper and Detection.

5.1.4.6.3 Scanning/Malicious code (Optical Media/SW/Scan Info Systems)

Contractor or Sub-Contractor will use reasonable efforts to investigate whether computer viruses or malware is present in any software or patches before providing such software or patches to USDA. Refer to Section 5.1.4.2.2 - Viruses and Malware.

5.1.4.7 Deployment

5.1.4.7.1 System Configuration

Contractor or Sub-Contractor is responsible for system configuration (i.e. System hardening) and must comply with the USDA C2 level of security (based on the NSA Trusted Computer Security Evaluation Criteria) for all USDA IT Systems. System hardening, or C2, as defined by the NSA, includes making specific modifications to an operating system before it is put into use to aid in the reduction of operating risks and to increase system availability, confidentiality and integrity. In addition, Contractor or Sub-Contractor will comply to DISA Security Technical Implementation Guide (STIG).

5.1.4.8 Operation and Maintenance

5.1.4.8.1 Continuous Monitoring

Contractor/Sub-Contractor] will provide ongoing agency system security, vulnerability, and threat awareness to USDA in accordance with Risk Management Framework (RMF) process. Continuous monitor and support agency IT system Authorization to Operate (ATO) submissions. Monitor IT network, information, and system security. Contractor or Sub-Contractor's continuous monitoring practices shall comply with USDA DR 3505-005 - *Cybersecurity Incident Management.*

5.1.4.9 Return USDA Government Furnished Property

5.1.4.9.1 Chain of Custody

Chain of Custody apply throughout the ICT SCRM SDLC phases; therefore, refer to Section 5.1.5.1 – Chain of Custody.

5.1.4.9.2 Anti-Tamper Testing/Inspection

Tamper Resistance and Detection apply throughout the ICT SCRM SDLC phases; therefore, refer to Section 5.1.5.2 – Anti-Tamper and Detection.

5.1.4.9.3 Return of Government Furnished Property

Government furnished property (GFP) is property that is furnished to a contractor for performance of a USDA contract. There are two types of Government Furnished Property: Equipment and Material. Upon completion of the contract, [Contract/Vendor] is required to follow return of GFP in accordance with the latest publication of NIST 800-88 - *Guidelines for Media Sanitization* and compliance in with best industry practices such as Department of Defense 5220-22-M Standard - *National Industrial Security Program (NISP).*

Upon completion of the delivery of the products and services to be provided under this Agreement, or at any time upon USDA's request, Contractor or Sub-Contractor will return to USDA all hardware and removable media provided by USDA containing USDA Information. USDA Information in returned hardware and removable media shall not be removed or altered in any way. The hardware should be physically sealed and returned via a bonded courier or as otherwise directed by USDA. If the hardware or removable media containing USDA Information is owned by Contractor or Sub-Contractor or a third-party, a notarized statement detailing the destruction method used and the data sets involved, the date of destruction, and the entity or individual who performed the destruction will be sent to a designated USDA security representative within fifteen (15) calendar days after completion of the delivery of the products and services to be provided under this Agreement, or at any time upon USDA's request. Contractor or Sub-Contractor's destruction or erasure of USDA Information pursuant to this Section shall comply with best industry practices (*e.g.*, Department of Defense 5220-22-M Standard, as may be amended). USDA will determine future disposition of government furnished equipment (i.e. disposal, recycle).

5.1.5 All-Inclusive Areas Within ICT SCRM SDLC

This section contains activities that apply throughout the ICT SCRM SDLC; therefore, Contractor or Sub-Contractor are to adhere to the all-inclusive areas without exception.

5.1.5.1 Chain of Custody

Contractor or Sub-Contractor is responsible for the end-to-end visibility and sensor technology that enables 24-7 monitoring of cargo which includes who touched it at either end; whether the cargo has deviated from its designated route; or whether the container or package has been opened in route. Sensors provide information on cargo conditions such as shock detectors, temperature, humidity, etc. These types of asset visibility measures safeguard both the physical security and quality of the shipment.

5.1.5.2 Tamper Resistance and Detection

Contractor or Sub-Contractor shall use a combination of hardware and software techniques for tamper resistance and detection. These techniques should include but not limited to obfuscation and self-checking to make reverse engineering and modifications more difficult, time-consuming, and expensive for adversaries. Strong identification combined with tamper resistance and/or tamper detection is essential to protecting information systems, components, and products during distribution and when in use.

5.1.5.3 Incidents

5.1.5.3.1 Vendor Identified Incidents

Whenever a security incident occurs, Contractor or Sub-Contractor agrees to notify USDA within # by telephone and email, and subsequently via written correspondence or form.

5.1.5.3.2 Incident Response

Upon any cyber incident, Contractor or Sub-Contractor will adhere to USDA DR 3505-005 - *Cybersecurity Incident Management.*

Within 3 days of notifying USDA of the security incident, Contractor or Sub-Contractor shall recommend actions to be taken by USDA on USDA-controlled systems to reduce the risk of a recurrence of the same or a similar security incident, including, as appropriate, the provision of action plans and mitigating controls. Contractor or Sub-Contractor shall coordinate with USDA in developing those action plans and mitigating controls. Contractor or Sub-Contractor will provide USDA guidance and recommendations for long term remediation of any cybersecurity risks posed to USDA information, equipment, systems, and networks as well as any information necessary to assist USDA in any recovery efforts undertaken by USDA in response to the security incident.

5.1.5.3.3 Development and Implementation of a Response Plan

Contractor or Sub-Contractor shall develop and implement policies and procedures to address security incidents (“Response Plan”) by mitigating the harmful effects of security incidents and remedying the occurrence to prevent the recurrence of security incidents in the future.

Contractor or Sub-Contractor shall provide USDA access to inspect its Response Plan. The development and implementation of the Response Plan shall follow best practices that at a minimum are consistent with the contingency planning requirements of the latest publication:

- NIST Special Publication 800-61 Rev. 2, Computer Security Incident Handling Guide
- NIST Special Publication 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations
    - CP-1 through CP-137
    - IR-1 through IR-10

Immediately upon learning of a security incident related to the products and services provided to USDA, Contractor or Sub-Contractor shall implement its Response Plan and within 24 hours of implementing its Response Plan, shall notify USDA.

5.1.5.3.4 Prevention of Recurrence:

Within 3 days of a security incident, Contractor or Sub-Contractor shall develop and execute a plan that reduces the likelihood of the same or a similar security incident from occurring in the future consistent with the requirements of its Response Plan and NIST Special Publication 800-61rev2 and NIST Special Publication 800-184, Guide for Cybersecurity Event Recovery (as may be amended) and shall communicate that plan to USDA. Contractor or Sub-Contractor shall provide recommendations to USDA on actions that USDA may take to assist in the prevention of recurrence, as applicable or appropriate.

5.1.5.3.5 Customer Notification (CN):

Contractor or Sub-Contractor will, at its sole cost and expense, assist and cooperate with USDA with respect to any investigation of a security incident, critical and high vulnerabilities and product flaws, disclosures to affected parties, and other remedial measures as requested by USDA in connection with a security incident or required under any applicable laws related to a Security Incident.

In the event a Security Incident results in USDA information being disclosed such that notification is required to be made to any person or entity, including without limitation any customer, shareholder, or current or former employee of USDA under any applicable laws, including privacy and consumer protection laws, or pursuant to a request or directive from a governmental authority, such notification will be provided by USDA, except as required by applicable law or approved by USDA in writing. USDA will have sole control over the timing and method of providing such notification.

5.1.5.4 Vulnerabilities

5.1.5.4.1 Disclosure and Remediation of Known Vulnerabilities by Vendor

Contractor or Sub-Contractor shall develop and implement policies and procedures to address the disclosure and remediation by Contractor or Sub-Contractor of vulnerabilities and material defects related to the products and services provided to USDA under this Agreement including the following:

a. Prior to the delivery of the procured product or service, Contractor or Sub-Contractor shall provide summary documentation of publicly disclosed vulnerabilities and material defects related in the procured product or services, the potential impact of such vulnerabilities and material defects, the status of Contractor or Sub-Contractor's efforts to mitigate those publicly disclosed vulnerabilities and material defects, and Contractor or Sub-Contractor's recommended corrective actions, compensating security controls, mitigations, and/or procedural workarounds.

b. Contractor or Sub-Contractor shall provide summary documentation of vulnerabilities and material defects in the procured product or services within thirty (30) calendar days after such vulnerabilities and material defects become known to Contractor or Sub-Contractor. This includes summary documentation on vulnerabilities that have not been publicly disclosed or have only been identified after the delivery of the product. The summary documentation shall include a description of each vulnerability and material defects and its potential impact, root cause, and recommended corrective actions, compensating security controls, mitigations, and/or procedural workarounds.

c. Contractor or Sub-Contractor shall disclose the existence of all known methods for bypassing computer authentication in the procured product or services, often referred to as backdoors, and provide written documentation that all such backdoors created by Contractor or Sub-Contractor have been permanently deleted or disabled.

d. Contractor or Sub-Contractor shall implement a vulnerability detection and remediation program consistent with the latest publication of NIST Special Publication 800-53 RA-5,18 SA-11/19 and SI-2 (as may be amended).

5.1.5.5 USDA's Audit Rights

USDA or its third-party designee may, but is not obligated to, perform audits and security tests of Contractor or Sub-Contractor's IT or systems environment and procedural controls to determine Contractor or Sub-Contractor's compliance with the system, network, data, and information security requirements of this Agreement. These audits and tests may include coordinated security tests, interviews of relevant personnel, review of documentation, and technical inspection of systems and networks as they relate to the receipt, maintenance, use, retention, and authorized destruction of USDA Information. Contractor or Sub-Contractor shall provide all information reasonably requested by USDA in connection with any such audits and shall provide reasonable access and assistance to USDA upon request. Contractor or Sub-Contractor will comply, within reasonable timeframes at its own cost and expense, with all reasonable recommendations that result from such inspections, tests, and audits. USDA reserves the right to view, upon request, any original security reports that Contractor or Sub-Contractor has undertaken or commissioned to assess Contractor or Sub-Contractor's own network security. If requested, copies of these reports will be sent via bonded courier to USDA security contact. Contractor or Sub-Contractor will notify USDA of any such security reports or similar assessments once they have been completed. Any regulators of USDA or its affiliates shall have the same rights of audit as described herein upon request.

Evidence of compliance or successful documented operational implementation can be in the form of inspection/audit results, or artifacts related to applicable Supply Chain or Information Security Management System certifications (e.g. O-TTPS/ISO 20243:2018), or internal SCRM program test/inspection results related to quality, security, or supplier management programs.

5.1.5.6 Covered Telecommunication Equipment or Services (Section 889(a)(1)(B))

In support of FAR Case 2019-009 on Section 889(a)(1)(B) of the John S. McCain National Defense Authorization Act (NDAA) commonly referred to as "Section 889 Part":

If the contractor confirms that it identified prohibited telecom used during contract performance and an existing waiver does not apply, the CO shall submit a Supply Chain Event Report to the SCRM Review Board, including, at a minimum:

(1) A "critical date", no less than three business days, for when a response from the SCRM Review Board is requested. The CO may proceed to the next step(s) below if the SCRM Review Board has not responded by the "critical date".

(2) The information provided by the offeror under paragraph (d) of the reporting clause at FAR 52.204-25.

(3) Be aware that the SCRM Review Board may ask for additional information.

5.1.5.6.1 Identified Prohibited Telecom

If the contractor confirms that it identified prohibited telecom used during contract performance and there is no applicable waiver, the CO will need to determine whether an exception applies, if the prohibited telecom is not a

substantial or essential component of a system, or if the prohibited telecom is not critical technology as part of any system.

1) The SCRM Review Board will provide to the CO, via response to the Supply Chain Event Report, information as to whether it thinks that continued performance or extension of the contract (or order) will result in a violation of the prohibition. If the SCRM Review Board has not responded by the "critical date", the CO may decide without the SCRM Review Board's input.
2) Resources for assisting the CO in making this determination, based on previous guidance provided by GSA's SCRM Review Board, will be available on the Acquisition Portal athttp://insite.gsa.gov/scrm.
3) If, after using such resources, the CO cannot make this determination on their own, the CO should consult with their acquisition team, technical experts, their management, and request additional assistance from the SCRM Review Board by contacting SCRM-Review-Board@gsa.gov.
4) If the CO determines that continued performance or extension of the contract (or order) will not result in a violation of the prohibition, the CO should document the file accordingly and may continue performance of and/or extend the contract (or order).

5.1.5.6.2 Exceptions Clarification

The statute includes two exceptions at 889 (a)(2)(A) and (B). (1) The exception at 889(a)(2)(A) allows the head of executive agency to procure with an entity "to provide a service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements". (2) The exception at 889(a)(2)(B) allows an entity to procure "telecommunications equipment that cannot route or redirect user data traffic or [cannot] permit visibility into any user data or packets that such equipment transmits or otherwise handles." **The exception allowing for procurement of services that connect to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements applies only to a Government agency that is contracting with an entity to provide a service**. **Therefore, the exception does not apply to a contractor's use of a service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements.** As a result, the Federal Government is prohibited from contracting with a contractor that uses covered telecommunications equipment or services to obtain backhaul services from an internet service provider, unless a waiver is granted.

5.1.5.7 Environmental Risks

Without proper risk aversion strategies, the supply chains can be disrupted by environmental factors; therefore, all the environment-related legislation made by governments and other regulatory bodies should be followed.

Negative environmental impacts such as carbon emissions can be reduced; waste must be disposed of properly; and chemicals handled properly to protect the environment. To avoid the dangers of natural disasters, Contractor or Sub-Contractor must choose their location and mode of transport strategically. They should be flexible and responsive enough to absorb changes and capable enough to avoid any distortions in the supply chain.

5.1.6 C-SCRM Appendices

5.1.6.1 Contractor or Sub-Contractor Cybersecurity Policy/System Security Plan

Contractor will provide to USDA the Contractor's cybersecurity policy or System Security Plan. The Contractor's cybersecurity policy shall be consistent with the latest publication of NIST Special Publications (SP) 800-39, NIST SP 800-37, as may be amended. The Contactor shall implement and comply with the cybersecurity policy. Any

changes to the Contactor's cybersecurity policy as applied to products and services provided to USDA under the contract and any USDA information that is inconsistent with the security requirements of the latest publication of NIST Special Publication 800-53 as may be amended shall be subject to review and approval by USDA prior to implementation by the Contractor.

The System Security Plan (SSP) contains information that is deemed non-disclosure, it contains the security posture of the system, the system diagrams, system interconnects, Topologies, system boundaries and all implemented and future controls to be implemented. It must be secured with enhancements.

5.1.6.2 Cybersecurity & Supply Chain Risk Management (SCRM) References

Contractors or Sub-Contractors entering into an agreement to provide service to Government activities are subject to cybersecurity and SCRM laws, regulations, policies, and reporting requirements. Additional and/or tailored cybersecurity and SCRM requirements may be included in individual Task Orders by the CO. The Contractor shall ensure all applicable Commercial-Off-The-Shelf (COTS), and enabled products comply with cybersecurity and SCRM requirements.

a. Laws
   - The Clinger-Cohen Act of 1996, Pub. L. 104-106, Division E
   - The Federal Information Security Modernization Act of 2014, Pub. L. 113-283
   - Federal Information Technology Acquisition Reform Act (FITARA), Pub. L.113-291
   - The SECURE Technology Act, Pub. L.115-390

b. Executive Orders
   - Executive Order 13859, Maintaining American Leadership in Artificial Intelligence
   - Executive Order 13873, Securing the Services and Communications Technology and Services Supply Chain
   - Executive Order 13833, Enhancing Effectiveness of Agency Chief Information Officers
   - Executive Order 13800, Strengthening Critical Infrastructure
   - Executive Order 13870, America's Cybersecurity Workforce

c. Policies of the Committee on National Security Systems
   - The policies presented under this topic address national security systems issues from abroad perspective. They establish national-level goals and objectives, all of which are binding upon all U.S. Government departments and agencies.
     - http://www.cnss.gov/CNSS/issuances/Policies.cfm

d. OMB Circulars and Memoranda
   - Circulars (https://www.whitehouse.gov/omb/information-for-agencies/circulars/)oA-130
     - A-123
     - A-108
     - A-11
   - •Memoranda (https://www.whitehouse.gov/omb/information-for-agencies/memoranda/)oM-19-18
     - M-19-17

- M-19-03
- M-19-02
- M-19-01
- M-18-23
- M-18-12
- M-17-25
- M-16-04
- M-15-14

e. National Institute of Standards and Technology (NIST)

- Federal Information Processing Standards (FIPS)
  - https://www.nist.gov/itl/fips-general-information
  - https://www.nist.gov/standardsgov/compliance-faqs-federal-information-processingstandards-fips
- Special Publication 800-series and 1800-seriesohttps://www.nist.gov/itl/nist-special-publication-800-series-general-information
  - https://csrc.nist.gov/publications/sp800
  - https://www.nist.gov/itl/nist-special-publication-1800-series-general-information
  - https://csrc.nist.gov/publications/sp1800
- Framework for Improving Critical Infrastructure
  - Cybersecurityohttps://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
- NICE Cybersecurity Workforce Framework Resource Center
  - https://www.nist.gov/itl/applied-cybersecurity/nice/nice-cybersecurity-workforceframework-resource-center

f. Cybersecurity and Infrastructure Security Agency

- Information and Communications Technology Supply Chain Risk Management

g. Cybersecurity Maturity Model Certification

- Cybersecurity Maturity Model Certification (CMMC)
- CMMC Accreditation Body

h. National Defense Authorization Act of 2019

- Section 881: Permanent Supply Chain Risk Management Authority
- Section 889: Prohibition on certain telecommunications and video surveillance services or equipment (FAR 52.204-24 and FAR 52.204-25)
- Sections 1631-1657: Cyber-spaced Related Matters

5.2 508 Requirements

Section 508 of the Rehabilitation Act, as amended by the Workforce Investment Act of 1998 (P.L. 105-220) requires that when Federal agencies develop, procure, maintain, or use information and communication technology (ICT), it shall be accessible to people with disabilities. Federal employees and members of the public who have disabilities must have access to, and use of, information and data that is comparable to people without disabilities.

E205 Electronic Content

E205.1 General Electronic content shall comply with E205.

E205.2 Public Facing Electronic content that is public facing shall conform to the accessibility requirements specified in E205.4.

E205.3 Agency Official Communication Electronic content that is not public facing shall conform to the accessibility requirements specified in E205.4 when such content constitutes official business and is communicated by an agency through one or more of the following:

A. An emergency notification;

B. An initial or final decision adjudicating an administrative claim or proceeding;

C. An internal or external program or policy announcement;

D. A notice of benefits, program eligibility, employment opportunity, or personnel action;

E. A formal acknowledgement of receipt;

F. A survey questionnaire;

G. A template or form;

H. Educational or training materials; or

I. Intranet content designed as a Web page.

E205.4 Accessibility Standard (WCAG 2.0) - Electronic content shall conform to Level A and Level AA Success Criteria and Conformance Requirements in WCAG 2.0 (Incorporated by reference, see 702.10.1).

E206 Hardware

E206.1 General. Where components of ICT are hardware and transmit information or have a user interface, such components shall conform to the requirements in Chapter 4.

E207 Software

E207.1 General Where components of ICT are software and transmit information or have a user interface, such components shall conform to E207 and the requirements in Chapter 5

Exception from E207.1 General: Software that is assistive technology and that supports the accessibility services of the platform shall not be required to conform to the requirements in Chapter 5.

E207.2 WCAG Conformance User interface components, as well as the content of platforms and applications, shall conform to Level A and Level AA Success Criteria and Conformance Requirements in WCAG 2.0 (incorporated by reference, see 702.10.1).

Exceptions from E207.2 WCAG Conformance:

Software that is assistive technology and that supports the accessibility services of the platform shall not be required to conform to E207.2.

Non-web software shall not be required to conform to the following four Success Criteria in WCAG 2.0: 2.4.1 Bypass Blocks; 2.4.5 Multiple Ways; 3.2.3 Consistent Navigation; and 3.2.4 Consistent Identification.

Non-Web software shall not be required to conform to Conformance Requirement 3 Complete Processes in WCAG 2.0.

E207.3 Complete Process for Non-Web Software Where non-Web software requires multiple steps to accomplish an activity, all software related to the activity to be accomplished shall conform to WCAG 2.0 as specified in E207.2.

E208 Support Documentation and Services

E208.1 General Where an agency provides support documentation or services for ICT, such documentation and services shall conform to the requirements in Chapter 6.

E301 General

E301.1 Scope. The requirements of Chapter 3 shall apply to ICT where required by 508 Chapter 2 (Scoping Requirements), 255 Chapter 2 (Scoping Requirements), and where otherwise referenced in any other chapter of the Revised 508 Standards or Revised 255 Guidelines.

E302 Functional Performance Criteria

302.1 Without Vision. Where a visual mode of operation is provided, ICT shall provide at least one mode of operation that does not require user vision.

302.2 With Limited Vision. Where a visual mode of operation is provided, ICT shall provide at least one mode of operation that enables users to make use of limited vision.

302.3 Without Perception of Color. Where a visual mode of operation is provided, ICT shall provide at least one visual mode of operation that does not require user perception of color.

302.4 Without Hearing. Where an audible mode of operation is provided, ICT shall provide at least one mode of operation that does not require user hearing.

302.5 With Limited Hearing. Where an audible mode of operation is provided, ICT shall provide at least one mode of operation that enables users to make use of limited hearing.

302.6 Without Speech. Where speech is used for input, control, or operation, ICT shall provide at least one mode of operation that does not require user speech.

302.7 With Limited Manipulation. Where a manual mode of operation is provided, ICT shall provide at least one mode of operation that does not require fine motor control or simultaneous manual operations.

302.8 With Limited Reach and Strength. Where a manual mode of operation is provided, ICT shall provide at least one mode of operation that is operable with limited reach and limited strength.

302.9 With Limited Language, Cognitive, and Learning Abilities. ICT shall provide features making its use by individuals with limited cognitive, language, and learning abilities simpler and easier.

503 Applications

503.1 General Applications shall conform to 503.

503.2 User Preferences Applications shall permit user preferences from platform settings for color, contrast, font type, font size, and focus cursor.

Exception from E503.2 User Preferences: Applications that are designed to be isolated from their underlying platform software, including Web applications, shall not be required to conform to 503.2.

503.3 Alternative User Interfaces. Where an application provides an alternative user interface that functions as assistive technology, the application shall use platform and other industry standard accessibility services.

503.4 User Controls for Captions and Audio Description Where ICT displays video with synchronized audio, ICT shall provide user controls for closed captions and audio descriptions conforming to 503.4.

503.4.1 Caption Controls Where user controls are provided for volume adjustment, ICT shall provide user controls for the selection of captions at the same menu level as the user controls for volume or program selection.

503.4.2 Audio Description Controls. Where user controls are provided for program selection, ICT shall provide user controls for the selection of audio descriptions at the same menu level as the user controls for volume or program selection.

504 Authoring Tools

504.2 Content Creation or Editing Authoring tools shall provide a mode of operation to create or edit content that conforms to Level A and Level AA Success Criteria and Conformance Requirements in WCAG 2.0 (incorporated by reference, see 702.10.1) for all supported features and, as applicable, to file formats supported by the authoring tool. Authoring tools shall permit authors the option of overriding information required for accessibility.

504.2.1 Preservation of Information Provided for Accessibility in Format Conversion. Authoring tools shall, when converting content from one format to another or saving content in multiple formats, preserve the information required for accessibility to the extent that the information is supported by the destination format.

504.2.2 PDF Export. Authoring tools capable of exporting PDF files that conform to ISO 32000-1:2008 (PDF 1.7) shall also be capable of exporting PDF files that conform to ANSI/AIIM/ISO 14289-1:2016 (PDF/UA-1) (incorporated by reference, see 702.3.1).

504.3 Prompts. Authoring tools shall provide a mode of operation that prompts authors to create content that conforms to Level A and Level AA Success Criteria and Conformance Requirements in WCAG 2.0 (incorporated by reference, see 702.10.1) for supported features and, as applicable, to file formats supported by the authoring tool.

504.4 Templates. Where templates are provided, templates allowing content creation that conforms to Level A and Level AA Success Criteria and Conformance Requirements in WCAG 2.0 (incorporated by reference, see 702.10.1) shall be provided for a range of template uses for supported features and, as applicable, to file formats supported by the authoring tool.

602 Support Documentation

602.1 General. Documentation that supports the use of ICT shall conform to 602.

602.2 Accessibility and Compatibility Features. Documentation shall list and explain how to use the accessibility and compatibility features required by Chapters 4 and 5. Documentation shall include accessibility features that are built-in and accessibility features that provide compatibility with assistive technology.

602.3 Electronic Support Documentation. Documentation in electronic format, including Web-based self-service support, shall conform to Level A and Level AA Success Criteria and Conformance Requirements in WCAG 2.0 (incorporated by reference, see 702.10.1).

602.4 Alternate Formats for Non-Electronic Support Documentation. Where support documentation is only provided in non-electronic formats, alternate formats usable by individuals with disabilities shall be provided upon request.

603 Support Services

603.1 General. ICT support services including, but not limited to, help desks, call centers, training services, and automated self-service technical support, shall conform to 603.

603.2 Information on Accessibility and Compatibility Features. ICT support services shall include information on the accessibility and compatibility features required by 602.2.

603.3 Accommodation of Communication Needs. Support services shall be provided directly to the user or through a referral to a point of contact. Such ICT support services shall accommodate the communication needs of individuals with disabilities.

5.3 Compliance with Internet Protocol Version 6 (IPv6)

Any system, hardware, software, firmware or networked component (voice, video or data) developed, procured or acquired in support or performance of this contract shall be capable of transmitting, receiving, processing, forwarding and storing digital information across system boundaries utilizing system packets that are formatted in accordance with commercial standards of Internet Protocol (IP) version 6 (IPv6) as set forth in the USGv6 Profile (NIST Special Publication 500-267) and corresponding declarations of conformance defined in the USGv6 Test Program. In addition, this system shall maintain interoperability with IPv4 systems and provide at least the same level of performance and reliability capabilities of IPv4 products:

- Specifically, any new IP product or system developed, acquired, or produced must:
  - Interoperate with both IPv6 and IPv4 systems and products, and
  - Have available contractor/vendor IPv6 technical support for development and implementation and fielded product management.
- As IPv6 evolves, the Contractor commits to upgrading or providing an appropriate migration path for each item developed, delivered or utilized at no additional cost to the Government.
- The Contractor shall provide technical support for both IPv4 and IPv6.
- Any system or software must be able to operate on networks supporting IPv4, IPv6 or one that supports both.
- Any product whose non-compliance is discovered and made known to the Contractor within one year after acceptance shall be upgraded, modified or replaced to bring it into compliance at no additional cost to the Government

5.4 Data Rights

5.4.1 Data collected, generated or managed

The Contractor shall be responsible for properly protecting all information used, gathered, or developed because of work under this task. The Contractor shall also protect all unclassified Government data, equipment, etc., by

treating information as sensitive business, confidential information, controlling and limiting access to the information, and ensuring the data and equipment are secured within their facility.

To the extent required to carry out a program of inspection to safeguard against threats and hazards to the security, integrity, and confidentiality of Government data, the Contractor will afford the Government access to the Contractor's or other external organization's facilities, installations, technical capabilities, operations, documentation, records, and databases. The Contractor will cooperate with Federal agencies and their officially credentialed representatives during official inspections or investigations concerning the protection of USDA information.

Cooperation may include providing relevant documentation showing proof of compliance with federal and agency requirements and rendering other assistance as deemed necessary.

5.4.2 Privacy Act

The Contractor Agrees To –

- Comply with the Privacy Act of 1974 (the Act) and the agency rules and regulations issued under the Act in the design, development, or operation of any system of records on individuals to accomplish an agency function when the contract specifically identifies—
    - The systems of records; and
    - The design, development, or operation work that the contractor is to perform;
- Include the Privacy Act notification contained in this contract in every solicitation and resulting subcontract and in every subcontract awarded without a solicitation, when the work statement in the proposed subcontract requires the redesign, development, or operation of a system of records on individuals that is subject to the Act; and
- Include this clause, including this paragraph, in all subcontracts awarded under this contract, which requires the design, development, or operation of such a system of records.
- In the event of violations of the Act, a civil action may be brought against the agency involved when the violation concerns the design, development, or operation of a system of records on individuals to accomplish an agency function, and criminal penalties may be imposed upon the officers or employees of the agency when the violation concerns the operation of a system of records on individuals to accomplish an agency function. For purposes of the Act, when the contract is for the operation of a system of records on individuals to accomplish an agency function, the Contractor is considered to be an employee of the agency.
- Definitions of the clause:
    - "Operation of a system of records," as used in this clause, means performance of any of the activities associated with maintaining the system of records, including the collection, use, and dissemination of records.
    - "Record," as used in this clause, means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and that contains the person's name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a fingerprint or voiceprint or a photograph.

5.4.3 Confidentiality and Non-Disclosure

Any USDA proprietary information, data, and/or equipment that the Contractor has been granted access by USDA to perform work under this order, will be returned to the USDA when no longer required to perform work under this order. The public release of USDA proprietary information must be authorized in writing by the Contracting Officer.

The component parts of this effort and reports are expected to contain highly sensitive information that may act as a guide for hostile entities to cause harm to the Department's critical infrastructure. Any such information made available in any format shall be used only for the purpose of carrying out the provisions of this agreement. Such information shall not be divulged or made known in any manner to any person.

The Contractor shall immediately notify the Contractor Program Manager, the Contractor on-site Manager, the COR, the Government TPM and the Contracting Officer upon discovery of any inadvertent disclosures of information. The Contractor shall not retain any information regarding vulnerabilities, to include summaries, the actual vulnerability report, etc., at the end of the task order. All information arising from this task, both hard copy and electronic, shall be returned to the COR and Government TPM at task completion.

The Contractor must agree that:

- The draft and final deliverables and all associated working papers and other materials deemed relevant by the USDA TPMs that have been generated by the Contractor in the performance of this task order are the property of the U.S. Government and must be submitted to the USDA TPMs at the conclusion of the tasks.
- All documents produced for this project are the property of the U.S. Government and cannot be reproduced or retained by the Contractor. All appropriate project documentation will be given to the Government TPM during and at the end of this contract. The Contractor will release no information. Any request for information relating to this Statement of Work presented to the Contractor must be submitted in writing to the USDA TPMs and the CO, who in turn will 12.3 under assignment of this contract.

5.4.4 Sensitive Information Storage and Disclosure

Sensitive information, data, and/or equipment will be disclosed only to authorize personnel on a Need-To-Know basis. The holder shall ensure that appropriate administrative, technical, and physical safeguards are established to ensure the security and confidentiality of this information, data, and/or equipment will be returned to Government control; destroyed; or held until otherwise directed. Destruction of items shall be accomplished by tearing into small parts; burning; shredding or other method that precludes the reconstruction of the material.

Work on this contract may require that personnel have access to Privacy Information. Personnel 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 take the required USDA Security Awareness and Rules of Behavior Training.

5.4.5 Release of Information

No USDA data shall be divulged to any unauthorized person, for any purpose. Therefore, the Contractor shall clear with the Contracting Officer any public release of any information. Information includes news stories, articles, sales and marketing information, advertisements, etc. All requests for public release of information shall

be submitted via email to the COR and Government Technical Program Manager (TPM) and the Contracting Officer and addressed to:

United States Department of Agriculture

Office of Communications (OC)

1400 Independence Avenue, SW

Washington, DC 20250

The Contracting Officer shall submit the Contractor's Request for Press Release to the Office of Communications (OC) for approval. The Contractor shall not release any information to the public without official OC approval from the Contracting Officer.

5.4.6 Return of Data

Data and information developed, entered, and processed under this contract shall be considered Government property. All data and/or materials provided to the contractor to accomplish individual deliverables, or data generated as a result of accomplishing individual deliverables, shall be returned to the Government or destroyed at the end of each applicable deliverable, unless the contractor specifically requests and receives approval from the COR to maintain copies of this data. The Contractor is responsible for distributing data and/or materials given to members of the contractor's team. None of this data will be released to any other Government organization or other organizations of individuals without the express written approval of USDA unless otherwise specified.

5.5 Privacy Act

5.5.1 Privacy Act Notification (Apr 1984)

The Contractor will be required to design, develop, or operate a system of records on individuals, to accomplish an agency function subject to the Privacy Act of 1974, Public Law 93-579, December 31, 1974 (5 U.S.C. 552a) and applicable agency regulations. Violation of the Act may involve the imposition of criminal penalties.

5.5.2 Privacy Act (Apr 1984)

a. The Contractor agrees to-

1. Comply with the Privacy Act of 1974 (the Act) and the agency rules and regulations issued under the Act in the design, development, or operation of any system of records on individuals to accomplish an agency function when the contract specifically identifies-

    i. The systems of records; and

    ii. The design, development, or operation work that the contractor is to perform;

2. Include the Privacy Act notification contained in this contract in every solicitation and resulting subcontract and in every subcontract awarded without a solicitation, when the work statement in the proposed subcontract requires the redesign, development, or operation of a system of records on individuals that is subject to the Act; and

3. Include this clause, including this paragraph (3), in all subcontracts awarded under this contract which requires the design, development, or operation of such a system of records.

b. In the event of violations of the Act, a civil action may be brought against the agency involved when the violation concerns the design, development, or operation of a system of records on individuals to accomplish an agency function, and criminal penalties may be imposed upon the officers or employees of the agency when the violation concerns the operation of a system of records on individuals to accomplish an agency function. For purposes of the Act, when the contract is for the operation of a system of records on individuals to accomplish an agency function, the Contractor is considered to be an employee of the agency.

c. Definitions

1. "Operation of a system of records," as used in this clause, means performance of any of the activities associated with maintaining the system of records, including the collection, use, and dissemination of records.

2. "Record," as used in this clause, means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and that contains the person's name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a fingerprint or voiceprint or a photograph.

3. "System of records on individuals," as used in this clause, means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

5.5.3 Privacy Training (JAN 2017)

a. Definition. As used in this clause, "personally identifiable information" means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. (See Office of Management and Budget (OMB) Circular A-130, Managing Federal Information as a Strategic Resource).

b. The Contractor shall ensure that initial privacy training, and annual privacy training, thereafter, is completed by contractor employees who-

(1) Have access to a system of records;

(2) Create, collect, use, process, store, maintain, disseminate, disclose, dispose, or otherwise handle personally identifiable information on behalf of an agency; or

(3) Design, develop, maintain, or operate a system of records (see also FAR subpart 24.3 and 39.105).

c.

(1) "Privacy training shall address the key elements necessary for ensuring the safeguarding of personally identifiable information or a system of records. The training shall be role-based, provide foundational as well as more advanced levels of training, and have measures in place to test the knowledge level of users. At a minimum, the privacy training shall cover-

i. The provisions of the Privacy Act of 1974 (5 U.S.C. 552a), including penalties for violations of the Act;

ii. The appropriate handling and safeguarding of personally identifiable information;

iii. The authorized and official use of a system of records or any other personally identifiable information;

iv. The restriction on the use of unauthorized equipment to create, collect, use, process, store, maintain, disseminate, disclose, dispose or otherwise access personally identifiable information.

v. The prohibition against the unauthorized use of a system of records or unauthorized disclosure, access, handling, or use of personally identifiable information; and

vi. The procedures to be followed in the event of a suspected or confirmed breach of a system of records or the unauthorized disclosure, access, handling, or use of personally identifiable information (see OMB guidance for Preparing for and Responding to a Breach of Personally Identifiable Information).

(2) Completion of an agency-developed or agency-conducted training course shall be deemed to satisfy these elements.

d. The Contractor shall maintain and, upon request, provide documentation of completion of privacy training to the Contracting Officer.

e. The Contractor shall not allow any employee access to a system of records, or permit any employee to create, collect, use, process, store, maintain, disseminate, disclose, dispose or otherwise handle personally identifiable information, or to design, develop, maintain, or operate a system of records unless the employee has completed privacy training, as required by this clause.

f. The substance of this clause, including this paragraph (f), shall be included in all subcontracts under this contract, when subcontractor employees will-

(1) Have access to a system of records;

(2) Create, collect, use, process, store, maintain, disseminate, disclose, dispose, or otherwise handle personally identifiable information; or

(3) Design, develop, maintain, or operate a system of records.

Resources: Federal Acquisition Regulations (FAR) Privacy Act provisions (Subparts 24.1 and 24.2) and include the specified contract clauses (52.224 Parts 52.224-1 and 52.224-2) Alternate I (JAN 2017). As prescribed in 24.302(b), if the agency specifies that only its agency-provided training is acceptable, substitute the following paragraph (c) for paragraph (c) of the basic clause:

(c) The contracting agency will provide initial privacy training, and annual privacy training thereafter, to Contractor employees for the duration of this contract.

5.6 Technical Guidance

The following documents (versions current at time of award) are incorporated with the same force and effect as if provided in full text. Succeeding revisions may be substituted or incorporated as required with full notice and disclosure to the Contractor. The Government will provide access to available documents and technical information as required and upon Contractor request for the performance of this PWS.

FPAC Technical Guidance Framework (TGF)

Level 1: Policies, Mandates, Directives, Decisions

Level 2: Strategies, Patterns, AoAs, Reference Architecture, Playbooks

Level 3: Technology Catalogs, Code Scanners, Security Scanners, Testing Tools, Dashboards

FPAC Security Standards

System Specifications, including all application-specific configurations

Other policy, procedural, or technical documentation as the Government may deem necessary to conduct work under this contract.

6 Performance Requirements Summary

PWS Reference	Requirement/ Deliverable Description	Deliverable Format	Deliverable Due /Frequency	Performance Standard	Acceptable Quality Levels (AQL) %	Surveillance Frequency	Method Surveillance	Remedy
List the PWS reference number	Provide summary of requirement from PWS that must be accomplished for the desired result.	Provide the format the government requires for the deliverable	Provide when the deliverable is due/on what frequency the requirement/ deliverable is required by the government	Provide the government's timelines/quality expectations as it relates to the requirement/ deliverable	Provide the % of the time the quality/timeliness standard needs to be met. Only use 100% in critical/no errors ever allowed/ acceptable type of situations	Provide how often the government wants to be able to surveil? For example, daily, weekly, monthly, quarterly, annual, as needed, as determined by the government, as examples	Provide how the government will surveil. For example, 100% Inspection, Random Sampling, or Customer Feedback- can also add more specifics after indication of one of the three typical methods	Provide the expected resolution time if errors/issues/ problems are identified during surveillance

7 Acronyms