SOLICITATION/CONTRACT/ORDER FOR COMMERCIAL ITEMS
OFFEROR TO COMPLETE BLOCKS 12, 17, 23, 24, & 30

1. REQUISITION NUMBER	PAGE	OF
	1	3

2. CONTRACT NO.	3. AWARD/ EFFECTIVE DATE	4. ORDER NUMBER	5. SOLICITATION NUMBER	6. SOLICITATION ISSUE DATE
12314420A0034			12314420Q0048	09/04/2020

7. FOR SOLICITATION INFORMATION CALL:	a. NAME	b. TELEPHONE NUMBER (No collect calls)	8. OFFER DUE DATE/LOCAL TIME
	MONICA TAYLOR	202-720-3009	

9. ISSUED BY — CODE: DASO-OCP-POD-

USDA, DM/OCP/POD/AMB, POD Acq Mgmt
Acquisition Management Branch-CO
301 S. Howes St., Suite 321
Fort Collins CO 80521-2795

10. THIS ACQUISITION IS ☒ UNRESTRICTED OR ☐ SET ASIDE: % FOR:

☐ SMALL BUSINESS
☐ HUBZONE SMALL BUSINESS
☐ SERVICE-DISABLED VETERAN-OWNED SMALL BUSINESS
☐ WOMEN-OWNED SMALL BUSINESS (WOSB) ELIGIBLE UNDER THE WOMEN-OWNED SMALL BUSINESS PROGRAM
☐ EDWOSB
☐ 8(A)

NAICS: 541519
SIZE STANDARD: $30.0

11. DELIVERY FOR FOB DESTINATION UNLESS BLOCK IS MARKED ☐ SEE SCHEDULE	12. DISCOUNT TERMS	☐ 13a. THIS CONTRACT IS A RATED ORDER UNDER DPAS (15 CFR 700)	13b. RATING / 14. METHOD OF SOLICITATION ☐RFQ ☐IFB ☐RFP
	As Indicated On Each Call		

15. DELIVER TO — CODE:

As Indicated On Each Call

16. ADMINISTERED BY — CODE: DASO-OCP-POD-AME

USDA, DM/OCP/POD/AMB, POD Acq Mgmt
Acquisition Management Branch-CO
301 S. Howes St., Suite 321
Fort Collins CO 80521-2795

17a. CONTRACTOR/ OFFEROR — CODE: 1100046778# — FACILITY CODE:

DELOITTE CONSULTING LLP - 0191215860000
DELOITTE CONSULTING LLP SUITE 800
1919 N. LYNN STREET
1100046778#
ARLINGTON VA 22209-1742

TELEPHONE NO.

18a. PAYMENT WILL BE MADE BY — CODE:

As Indicated On Each Call

☐ 17b. CHECK IF REMITTANCE IS DIFFERENT AND PUT SUCH ADDRESS IN OFFER

18b. SUBMIT INVOICES TO ADDRESS SHOWN IN BLOCK 18a UNLESS BLOCK BELOW IS CHECKED ☐ SEE ADDENDUM

19. ITEM NO.	20. SCHEDULE OF SUPPLIES/SERVICES	21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT
	GSA Contract #: GS-35F-0617Y Tax ID Number: 06-1454513 DUNS Number: 019121586 Salesforce Portal Development and Support Services Multiple-Award Federal Supply Schedule BPA This is a GSA Federal Supply Schedule Multiple-Award Blanket Purchase Agreement (BPA) for agile Salesforce Portal Development and Support Services. The multiple-award BPA numbers are as follows: 12314420A0032; 12314420A0033; *(Use Reverse and/or Attach Additional Sheets as Necessary)*				

25. ACCOUNTING AND APPROPRIATION DATA
As Indicated On Each Call

26. TOTAL AWARD AMOUNT *(For Govt. Use Only)*
$0.00

☐ 27a. SOLICITATION INCORPORATES BY REFERENCE FAR 52.212-1, 52.212-4. FAR 52.212-3 AND 52.212-5 ARE ATTACHED. ADDENDA ☐ ARE ☐ ARE NOT ATTACHED.
☒ 27b. CONTRACT/PURCHASE ORDER INCORPORATES BY REFERENCE FAR 52.212-4. FAR 52.212-5 IS ATTACHED. ADDENDA ☒ ARE ☐ ARE NOT ATTACHED.

☒ 28. CONTRACTOR IS REQUIRED TO SIGN THIS DOCUMENT AND RETURN 1 COPIES TO ISSUING OFFICE. CONTRACTOR AGREES TO FURNISH AND DELIVER ALL ITEMS SET FORTH OR OTHERWISE IDENTIFIED ABOVE AND ON ANY ADDITIONAL SHEETS SUBJECT TO THE TERMS AND CONDITIONS SPECIFIED.

☒ 29. AWARD OF CONTRACT: _____ OFFER DATED _____. YOUR OFFER ON SOLICITATION (BLOCK 5), INCLUDING ANY ADDITIONS OR CHANGES WHICH ARE SET FORTH HEREIN, IS ACCEPTED AS TO ITEMS:

30a. SIGNATURE OF OFFEROR/CONTRACTOR	31a. UNITED STATES OF AMERICA *(SIGNATURE OF CONTRACTING OFFICER)*
	

30b. NAME AND TITLE OF SIGNER *(Type or print)*	30c. DATE SIGNED	31b. NAME OF CONTRACTING OFFICER *(Type or print)*	31c. DATE SIGNED
		MONICA L. TAYLOR	09/28/2020

19. ITEM NO.	20. SCHEDULE OF SUPPLIES/SERVICES	21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT
	12314420A0034; and 12314420A0035. Orders are to be issued in accordance with the FAR BPA terms and conditions. Any warranted Contracting Officer within USDA, Procurement Operations Division can place call orders in accordance with FAR 8.405-3, BPAs, agency guidelines, and procurement regulations. This is an office-wide BPA. Contracting Officers must receive written concurrence from the BPA Contracting Officer prior to placement of an order. This BPA does not prohibit the Contractor(s) from offering additional discounts (e.g., quality, volume, cumulative) on a procurement specific basis. This BPA is not a binding contract. The parties are bound when and if a Call Order is issued under this agreement. See BPA attachments for additional details. Attachments -USDA Contract Clauses -BPA Ordering Terms and Performance Work Statement -FPAC Special IT Clauses -BPA Pricing Sheet (12314420A0034 Deloitte) Period of Performance: 09/29/2020 to 09/28/2025 Footer Text Contracting Officer: Monica L. Taylor, 202-720-3009, Continued ...				

32a. QUANTITY IN COLUMN 21 HAS BEEN

☐ RECEIVED ☐ INSPECTED ☐ ACCEPTED, AND CONFORMS TO THE CONTRACT, EXCEPT AS NOTED: _____

32b. SIGNATURE OF AUTHORIZED GOVERNMENT REPRESENTATIVE	32c. DATE	32d. PRINTED NAME AND TITLE OF AUTHORIZED GOVERNMENT REPRESENTATIVE

32e. MAILING ADDRESS OF AUTHORIZED GOVERNMENT REPRESENTATIVE	32f. TELEPHONE NUMBER OF AUTHORIZED GOVERNMENT REPRESENTATIVE
	32g. E-MAIL OF AUTHORIZED GOVERNMENT REPRESENTATIVE

33. SHIP NUMBER	34. VOUCHER NUMBER	35. AMOUNT VERIFIED CORRECT FOR	36. PAYMENT	37. CHECK NUMBER
☐ PARTIAL ☐ FINAL			☐ COMPLETE ☐ PARTIAL ☐ FINAL	

38. S/R ACCOUNT NUMBER	39. S/R VOUCHER NUMBER	40. PAID BY

41a. I CERTIFY THIS ACCOUNT IS CORRECT AND PROPER FOR PAYMENT		42a. RECEIVED BY *(Print)*	
41b. SIGNATURE AND TITLE OF CERTIFYING OFFICER	41c. DATE	42b. RECEIVED AT *(Location)*	
		42c. DATE REC'D *(YY/MM/DD)*	42d. TOTAL CONTAINERS

NAME OF OFFEROR OR CONTRACTOR
DELOITTE CONSULTING LLP - 0191215860000

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	MonicaL.Taylor@usda.gov Contracting Officer Representative: Michelle Jardine, 801-844-2909, Michelle.Jardine@usda.gov Contractor Point of Contact: Michelle L. Koval, Senior Contracts Manager, mkoval@deloitte.com --- A call order can include at a minimum one Functional Area or any combination of the following: Functional Area 1: UX Design, Business Analysis, Development, Integration and Post-Implementation Defect Resolution Support Functional Area 2: Data Management and Securitization Functional Area 3: Program Management Support, IT Product Management and Governance Functional Area 4: Systems Support, Release Management and Post-Implementation Maintenance Support See BPA for details.				

Contents

United States Department of Agriculture
Farm Production and Conservation
Salesforce Portal Development and Support Services
Multiple-Award Blanket Purchase Agreement
Performance Work Statement

1.0 GENERAL INFORMATION

Pursuant to FAR Part 8.4, Federal Supply Schedules, USDA is entering into a multiple-award Blanket Purchase Agreement (FAR Part 8.405-3) for agile Salesforce Portal Development and Support Services. The objective of this multiple-award Blanket Purchase Agreement (BPA) is to provide a fast and effective way to procure high-level salesforce services while streamlining the process. The multiple-award BPA holders are as follows:

BPA No. 12314420A0032	Accenture Federal Services LLC
BPA No. 12314420A0033	Acumen Solutions, Inc.
BPA No. 12314420A0034	Deloitte Consulting LLP
BPA No. 12314420A0035	Vsolvit LLC

This BPA does not prohibit the Contractor(s) from offering additional discounts (e.g., quality, volume, cumulative) on a procurement specific basis. This BPA is not a binding contract. The parties are bound when and if a Call Order is issued under this agreement.

1.1 Authorized BPA Users

Any warranted Contracting Officer within USDA, Procurement Operations Division can place call orders in accordance with FAR 8.405-3, BPAs, agency guidelines, and procurement regulations. This is an office-wide BPA. Contracting Officers must receive written concurrence from the BPA Contracting Officer prior to placement of an order. Upon placement of a call order, the Contracting Officer shall send a copy of the fully executed order to the BPA Contracting Officer Representative (COR) and the USDA Contracting Officer within two (2) business days.

1.2 BPA Term and Call Order Type

The term of this multiple-award BPA will be for a total of five (5) years. Firm Fixed Price (FFP) orders are preferred as stated in FAR 8.405-3(c)(3). Each order issued will have its own period of performance.

1.3 BPA Pricing

The multiple awardees will propose discounted rates under their GSA Federal Supply Schedule (FSS) labor categories. USDA is buying capacity and pricing at the call order level will be per iteration and/or scrum teams. Any applicable GSA labor categories automatically flow to this USDA multiple-award BPA.

2.0 PERFORMANCE WORK STATEMENT

2.1 Background

On May 11, 2017, the United States Secretary of Agriculture Sonny Perdue announced the reorganization of the USDA to better serve rural America. As a part of the reorganization, three USDA agencies – the Farm Service Agency (FSA), Natural Resources Conservation Service (NRCS), and Risk Management Agency (RMA) – were relocated under a newly-created FPAC mission area. The new mission area focuses on domestic agricultural issues and simplified service for the USDA's customers.

The USDA's FPAC mission area offers production and conservation tools, financial assistance, and technical advice along with commodity, lending, and disaster programs for America's farmers, ranchers, and private foresters. With offices that serve customers in every state and county, FPAC agency employees deliver personalized customer service locally to producers, a service valued by producers and partners alike. The reorganization brought similar resources, programs, and tools together for customers. Those digital resources include three agency websites and a wide range of user business applications, all in varying conditions and on different platforms. Among its web applications, NRCS hosts the NRCS Conservation Client Gateway (CCG), a secured web application through which a client, individual or business, can manage their conservation plans and contracts, through an integrated document management system, and a system of request management. FSA hosts Farm+ (Farm Plus), a secure web application through which a client, individual or business, can manage and meet reporting requirements and view, export and print farm records data, including maps, through a public facing web portal.

Online, customers and the USDA employees that serve those customers encounter inconsistent digital information and resources spread across agencies and built outside of current design and customer-centric best practices, often utilizing outdated technology causing significant delays in conducting business with USDA and general dissatisfaction overall.

Motivated by Secretary Purdue's vision to better serve rural America, the Farmers.gov Customer Experience Portal was established as a central location for the breadth of services provided by USDA FPAC. As it continues to expand, this platform of integrated services will provide USDA FPAC customers and the USDA employees who serve those customers with consistency in design and functionality throughout their digital experience. The portal ecosystem contains two parts: 1) The Farmers.gov website provides customers with open online informational materials and engagement opportunities with USDA; and 2) a Transactional Portal with self-service options and tools for external and internal USDA customers that is the focus of this document.

Farmers.gov interacts with dozens of backend systems and sources of record to provide value through the features delivered. USDA FPAC has deployed more than 50 functional releases since 2018 across 20 major value streams. A few examples are illustrated below:

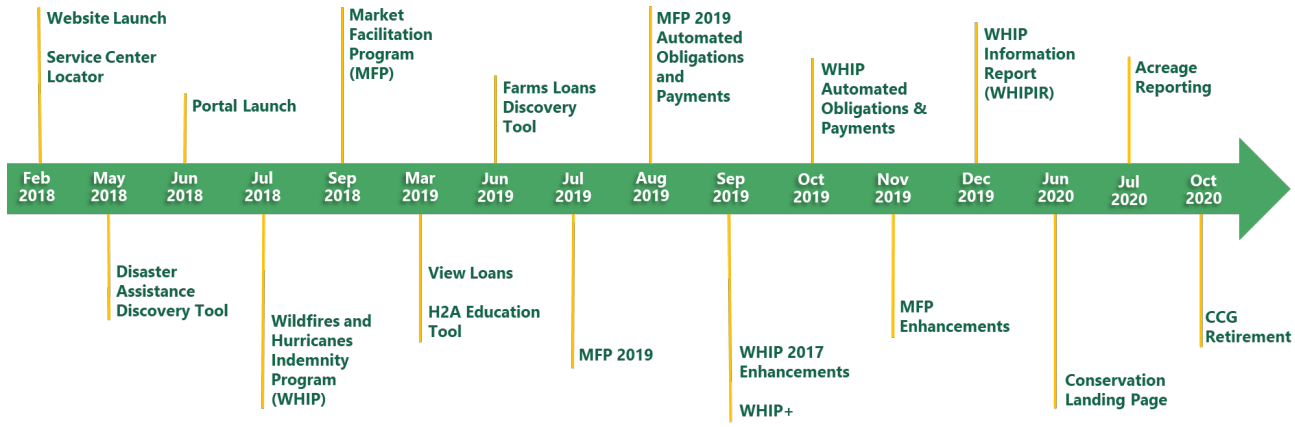

Figure 1: Farmers Past Production Releases

2.2 Objective

The objective of this BPA is to continually improve USDA FPAC customer and employee experience by continuing the integration of key business functions and services on Farmers.gov Customer Experience Portal built on Salesforce.com. The services procured under this BPA will be epitomized by driving towards the delivery of quality product within rapid time frames through the utilization of the Salesforce and MuleSoft platforms, and Esri tools to create applications with consistent architecture following standard Salesforce and MuleSoft development guidelines to promote reuse and shareability of all code and functionality across government in alignment with the Federal Digital Government Strategy 'Shared Platform Approach' to "build once, use many times".

2.3 Scope

The scope of this BPA encompasses requirements for providing platform strategy services, business process analysis, solution architecture and design, application development and configuration, implementation, release and enterprise environment management, and maintenance services required to successfully implement the Salesforce platform and applications to meet agency requirements.

The services provided under this BPA are for enterprise-level Salesforce partners with MuleSoft architects and Geospatial capability/experience who can manage implementations within complex, multi-org government cloud ecosystems. In some cases supporting more than 100 active applications and several thousand users. The complexity of the work requires that the service providers have proven Salesforce consulting capabilities, a strong past performance record and customer stories of the same scope, a bench of Certified Salesforce personnel, and the ability to manage large-scale, centralized releases and Agile development portfolios.

USDA intends to establish a multiple-award BPA for Salesforce-certified, MuleSoft, and Geospatial portal development and support services. Performance management information technology (IT) tools that are incidental to and in support of the implementation, integration, and support services may also be provided at the call order level.

The call orders to be issued under this multiple-award BPA will be based on scopes of work defining specific requirements.

2.4 Tasks

To fulfill the requirements of this multiple-award BPA, the contractors are expected to provide, but are not limited to, the following services. Call Orders placed under this BPA will specify which Functional Area(s) will be included in scope for each individual order. A call order can include at a minimum one Functional Area or any combination of the following:

Functional Area 1: UX Design, Business Analysis, Development, Integration and Post-Implementation Defect Resolution Support

Functional Area 2: Data Management and Securitization

Functional Area 3: Program Management Support, IT Product Management and Governance

Functional Area 4: Systems Support, Release Management and Post-Implementation Maintenance Support

2.4.1 *Functional Area 1: UX Design, Business Analysis, Development, Integration and Post-Implementation Defect Resolution Support -*

Creation of a technical architecture leading to the development of business applications, including integration with the existing systems. This includes expansion or updates to existing production applications to meet the ongoing, unique objectives and requirements of specific components.

Sample activities that would typically fall under Functional Area 1 are:

● Design solutions toward the end user experience so that products produced meet end user goals and measure of success as well as the strategic business objectives of the providing organization.

● Work with stakeholders and technology professionals to properly understand business requirements and develop an industry best practice approach to technology solutions;

●Provide subject matter expertise for the Salesforce Apex coding language;

●Develop, test, stage, and release business applications by applying iterative processes utilizing the proposed Agile methodology and a frequent release cycle;

●Provide customer-friendly open source solutions that provide ease of use for non-technical Government users;

●Ensure commercial best practices workflows shall come bundled with the solutions;

●Design solutions that offer role-based identity management, authorization, and authentication across all business applications;
●Ensure all content and activities are traceable to specific persons;
●Ensure all content is preserved according to federal record retention requirements, and applications have the ability to protect personally identifiable information (PII);
●Ensure applications are developed such that response times fall within acceptable limits;

●Provide secure mechanisms to allow data exchange and interaction with external systems through Application Programming Interfaces (APIs) or other methods;

●Provide business process analysis expertise with regard to optimizing the utilization and adoption of the software platform among government users;

●Seek to configure out-of-the-box aspects of the selected platform before recommending a customized coding approach to the maximum extent possible;

●Develop system configuration in such a manner as to leverage maximum re-use and sharing across the platform by other federal agencies;

●Provide full technical documentation for all software development efforts and product releases with all information necessary to document processes, procedures, code artifacts, and/or policies that were implemented in the creation of the development work;
●Include unified and comprehensive solution documentation for FSA features as standalone output.
●Include unified and comprehensive Wiki-style solution documentation for all features across the full development lifecycle within Confluence and Jira as applicable.

●Be equipped to support an enterprise-wide, multi-org Salesforce, Mulesoft & ESRI ecosystem, providing analysis and solution architecture recommendations considering functional overlap and reuse of objects or utilities;

●Rapidly deploy new or improved independent site features without requiring changes or downtime to unrelated site features;

●Design and implement system changes in a manner to support interoperability and scalability with future development efforts and in an open architecture manner;

●Allow the government to publish all source code or software artifacts for reuse in an open source manner;

2.4.2 *Functional Area 2: Data Management and Security* – Data management may include database architecture, data import/export tasks, data migration efforts, security with a Government provided third-party encryption tool, and creation of policy and/or procedures surrounding data implementation.

Sample activities that would typically fall under Functional Area 2 are:

●Provide database architecture subject matter expertise for the Salesforce and Force.com platforms;

●Include database performance and impact in all system design or development efforts to ensure industry best practices are supported;

●Work with third-party cloud encryption gateway technologies, if present, provided by the government to secure designated data while in transit to/from the cloud as well as at rest;

● Work with security in the creation of policy and/or procedures surrounding data implementation including the correction of application security vulnerabilities within 24 hours;

●Verify in writing to the Government that data migrated from any legacy system to the new Salesforce application is complete and accurate in accordance with the Federal Records Act and any other applicable federal law, according to the agreed upon framework coordinated with Agency and the Contractor and that all data is accessible;

●Be knowledgeable in data warehousing, data visualization and business intelligence best practices to provide guidance on data architecture and mapping;

●Provide systems and data integration and orchestration services between Salesforce and other systems of record or data warehouses using Mulesoft;

2.4.3 *Functional Area 3: Program Management Support, IT Product Management and Governance -* Provide the government program management, product management and governance support for managing applications on an enterprise-wide platform.

Sample activities that would typically fall under Functional Area 3 are:

●Give periodic project, program, product, and operational status updates as required by the government within an agreed-upon frequency and schedule. These

are typically bi-weekly agency program reviews and governance meetings along with call order status reports and weekly Agile/Scrum development meetings.

●Provide on-site project management support and attend in-person meetings on an ad-hoc basis.

●As part of the support, enterprise-wide platform architectural design, centralized design review of configuration and code prior to release, and support of the most current Salesforce / Force.com implementation best practices, features and functions.

●Provide project and operational documentation as required by the government to support specific project deliverables or ongoing operational support such as security Authority to Operate.

●Manage and oversee daily, weekly, and monthly workloads and schedule for active tasks with regard to schedule, budget, priority, risk, and quality to ensure quality response to government call order requests.

●Provide Product Management leadership that will lead cross-functional teams to deliver user-centered products using agile methodologies and modern software development practices while building capacity for product innovation in government. Coach agencies on modern product development practices so they're set up for success in the long term.

●Provide programmatic support for the agency's governing body, including application portfolio management and engagement with Enterprise Architecture, developing strategic roadmaps, creation of executive-level briefings, support in developing OMB capital planning reports, managing the new request intake and governance process, license management, and facilitating recurring program meetings.

2.4.4 *Functional Area 4: Release Management and Post-Implementation Maintenance Support* - Systems Support, Release Management and Post-Implementation Maintenance Support Enterprise-level management of releases from development to production and post-implementation operational and maintenance support of production applications on the platform.

Sample activities that would typically fall under Functional Area 4 are:

●Identify usability issues and craft solutions to resolve bug fixes or other performance problems;

●Advise and provide recommendations of how new manufacturer-driven updates of the platform shall be affected or upgraded according to manufacturer release schedules;

●Provide enterprise-wide release management support for large monthly releases, small configuration changes, and out-of-cycle emergency releases of code and configuration to higher environments, including production;

●Provide enterprise-wide release management support for incremental feature releases, configuration changes, and expedited code changes from development through production environments;

●Provide development environment management expertise, regression testing, and continuous integration management including the administration of the systems and tools that are used as part of that process.

2.5 Place of Performance

The performance location requirements will be identified at the call order level.

2.6 Skillsets/Key Capabilities

Skillsets of vendor resources for each call order may include, but are not limited to the following:

- **Salesforce Certified**: Salesforce platform development is among the greatest overall demand. This program requires technical architects that will be engaged in priority feature development such as Conservation, Farm Programs, Common Enablers, and RAP. Certified Technical Architects are required that will be directed by the Federal head of architecture for this program. All Salesforce Technical Architects are considered critical resources and are expected to be full time for the entire duration of the program. All efforts to minimize attrition in this area should be considered. Salesforce developers must be of the highest quality and greatest experience in order to handle the complexity and demand. They will be closely evaluated for performance, skills, and applied aptitude.
- **MuleSoft**: MuleSoft is the primary platform for integration with the FPAC ecosystem and critical path to the success of Farmers.gov. This program requires MuleSoft architects that will be under the direction of the Federal head of architecture for this program. All MuleSoft Architects are considered critical resources and are expected to be full time for the entire duration of the program. All efforts to minimize attrition in this area should be considered. MuleSoft developers must be of the highest quality and greatest experience in order to handle the complexity and demand. They will be closely evaluated for performance, skills, and applied aptitude.
- **Geospatial Information Systems (GIS)**: Geospatial functionality is among the most complex challenges faced to date and expected into the future for the Farmers.gov platform - from the way it is being integrated with Salesforce and MuleSoft to the

demands being made of the capabilities developed for end users. Strong experience and a depth of skills is required in this area with significant impact on the capabilities that can be delivered. As such, this program requires GIS architects that will be assigned as needed under the direction of the Federal head of architecture. All GIS Architects are considered critical resources and are expected to be full time for the entire duration of the program. All efforts to minimize attrition in this area should be considered. GIS developers must be of the highest quality and greatest experience in order to handle the complexity and demand. They are closely evaluated for performance, skills, and applied aptitude.

- **Program Leadership**: Farmers.gov is a complex platform with demands from multiple agencies and active political oversight. Demands for functionality come fast and furious, often requiring compromise. Demands can be legislatively, or strategic vision driven. The combination leads to a dynamic environment. Although Farmers.gov is implemented using SAFe as the primary methodology, this approach is relatively new to the federal government with adoption that is less then complete. There are many within the stakeholder community that will expect a more waterfall model at some level. Due to the level of investment, often the delivery team finds itself in a situation where time, cost, and scope are all fixed. Much of the functionality delivered through Farmers.gov is of limited value in MVP form requiring full functionality from the initial release. Tolerance to defects is low and stakeholders are willing to invest in quality, but 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. Program leadership must be adroit at dealing with all aspects illustrated above. Program leadership is part of critical path to success and considered key personnel that will be dedicated and full time at the call order level.

2.7 Guardrails

When using SAFe Agile methodologies, lean budget guardrails are to be established specific to the call order within the first program increment. Proposed and agreed upon guardrails must include an explanation of the guardrails and how they will be protected. Guardrails will be finalized in the call order Performance Work Statement by modification. Adjustment or change to the guardrails must be authorized by the call order Contracting Officer through a modification to the call order.

2.8 Additional Information Technology Requirements

Attachment B, FPAC Special IT Clauses, are USDA/FPAC specific requirements applicable to information technology acquisitions. These requirements are periodically updated, and the most recent version will be included with competed/awarded call orders. Refer to the attachment for requirements regarding Information Security, Personnel, Accessibility, Internet Protocol Version 6 (IPV6), Data Ownership, Non-Disclosure of Sensitive or Proprietary Information, Software

Line Item License Line Item Data, Government Furnished Property/Information Access, and Call order Administration. Attachment C, FPAC-BC SDLC, System Development Lifecycle Document, provides the framework and standard to guide the development and delivery of software solutions.

2.9 Performance Based Service

Performance-based call orders will be issued against this BPA and will include a mutually agreed upon Performance Work Statement incorporating the provided Statement of Objectives, as well as a mutually agreed upon Quality Assurance Surveillance Plan (QASP)/Service Level Agreement which may include, but not limited to standards covering the following:

- Delivery decrement due to attrition
- Velocity/Rate of functionality delivery
- Defects
- SAFe process implemented taking into account the agency's SAFe maturity level
- Building quality and testing into development to ensure minimum testing after user acceptance testing. This may include a rolling increase to unit test coverage per program increment from the current base of 81%, as well as standards for automated testing of 60-70%.
- Ensuring a clear definition of done that meets agreed upon functionality and quality.
- Delivery of up to 80 to 90% of capacity/functionality from user stories developed during PI (program increment) planning sessions.
- Supports rapid, cost effective development/modification of the operational system, training system, and support components to meet business user defined thresholds and as many stretch objectives as are affordable.
- Includes the ability to easily and inexpensively upgrade existing software and/or make use of existing components if available.
- Mitigates the risks associated with technology obsolescence, proprietary technologies, and reliance on a single source of supply over the life of the system.
- Risks to achieving functionality and deadline are clearly and timely communicated to Government product and business owners, program manager, sponsor, and agency leadership (when necessary) through agreed upon channels.
  Explanation of and adherence to lean budget guardrails critical to ensuring quality delivery and that expectations are met.

2.10 Expense Tracking and Reporting

Call orders may require expense tracking and reporting by major feature and value stream to ensure compliance with investment management and audits. Requirements will be described in call orders.

3.0 ADDITIONAL BPA REQUIREMENTS

3.1 BPA Annual Review

This BPA will be reviewed annually to determine whether it is in the best interest of the Government to continue use of this BPA. Either party, the government or the contractor, may cancel this BPA by providing written notice. The cancellation will take effect 30 calendar days after the other party receives the notice of cancellation. BPA cancellation does not release the BPA contractor from the duty to continue performance on existing orders. Ongoing orders will continue in accordance with their own period of performance, even if the BPA is cancelled.

3.2 Quarterly Status Report

The Quarterly Status Report (QSR) shall consist of high level and detailed information for each awarded call order. The BPA holder shall electronically update and submit the quarterly status report to the BPA Contracting Officer and COR containing the information below, using the format provided by the Contracting Officer or COR following award, if provided. Reports are to be submitted no later than fifteen (15) workdays after the end of each calendar year quarter. BPA holders with no call orders awarded during the quarter are required to submit an email notification to the BPA CO and COR stating that there is no quarterly status report. The status reports shall be cumulative, beginning from the time of BPA establishment, and include the following:

Call Order Report

- BPA No.
- Call Order No.
- Ordering Entity
- Call order Title
- Ordering CO name, phone number and email address
- Ordering Contracting Officer Representative name, phone number and email address
- Period of Performance (inclusive of base and options)
- Small Business subcontractor(s) (if applicable)
- Call Order Value for each small business subcontractor (if applicable)
- Order type
- Awarded call order price (inclusive of base and options)
- Total price at GSA schedule rates (with no discounts)
- Overall % discount
- Overall $ discount

Call Order Detail

- Call Order No./Line No.
- BPA task title (BPA SOW task area that encompasses call order work)
- GSA Schedule Contact Labor category Title
- GSA Schedule Contract # for labor category
- GSA Schedule Contract hourly rate (non-discounted rate)
- Call order hourly rate (discounted rate)

- Number of estimated hours
- Discount %

3.3 Quality Assurance

The performance of BPA contract holders will be measured in two contexts. One will be at the Call order level using quality metrics specific to the nature of the work required on the Call order. The Government may specify required metrics for a specific Call order Quality Assurance Surveillance Plan (QASP). The QASP will provide oversight help to ensure that the vendor's service levels reach and maintain the required levels for performance of the call order. The Vendor will provide a Quality Control Plan in response to each call/call order QASP. At the government's discretion, the government may determine it is in the best interest for the contractor to provide a Quality Assurance Surveillance Plan as a part of the proposal under the Call order. It is the Government's preference, when appropriate and practical, that performance information be provided via real-time tools (e.g. dashboards) made available to the Government rather than via separate paper or electronic reports.

Performance at the Call order level will also be measured in the categories of on-time delivery/schedule, cost control (if applicable), and management. Additionally, for Call orders that exceed the Simplified Acquisition Threshold, in order to meet Contractor Performance Information requirements in accordance with FAR Part 42.15, Contractor Performance Assessment Reporting System (CPARS) will be utilized. The Call order level QASP assessments will inform with those entered into CPARS. The second context will be for the evaluation of Past Performance at the Call order level. The Past Performance evaluations will be based upon input from the government to the Call order Contracting Officer Representative and Contracting Officer.

3.4 BPA Call Order(s) Transition-In/Transition-Out

Each Call order shall include transition-in/transition out as a part of its scope that may be more specifically prescribed at the call order level. During the transition-in period resources are being onboarded and knowledge transfer with the incumbent is taking place. Onboarding may require between four and eight weeks to receive a Security Initial Determination and Government Furnished Equipment required to work on USDA/FPAC systems. The ending performance period of call orders may also require similar knowledge transfer activities in order to successfully transition the performance to a new vendor. Performance of incoming and outgoing transition activities may be factored into the CPARS evaluation. The Vendor shall:

a) 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 this call order will be the property of the U.S. Government.

b) Within a designated period in the call order, provide a brief Transition Plan for all deliverables, products, and materials in coordination with the COR, Product Manager and Product Owner from FPAC.

c) Coordinate with the COR and potentially another vendor and implement the Transition Plan according to the COR's direction.

d) Assist the COR, Product Manager, and potentially other Government staff to stand-up any applications developed during the call order.

3.4.1 Transition Activities

During the transition to the Government, or a new vendor, the Vendor shall perform all necessary transition activities. Expected transition activities may include, but not be limited to, continuation of full services to FPAC Conservation and other customers; participation in meetings with the Government or new vendor to effect a smooth transition and provide detailed information on the operation of all deliverables, at COR's discretion; training of new personnel, either Government or new vendor, during transition period; and appropriate close-out of any outstanding technical and related performance elements for this task.

Final report shall include a list of sprint tasks completed, documentation, and link to code repository developed for Conservation. Should the Vendor be terminated prior to the end of the period of performance, the Vendor shall transfer all project materials to the COR within two weeks of the COR's request. Provide leadership and support for architecture and design of secure software applications and computer systems.

3.5 Travel

The Contractor may be required to support non-commuter travel in support of the call orders awarded against this BPA, as required by the Government. The Call order Contracting Officer and COR have 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 and schedule contract requirements. 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., Program Increment planning or specific workshops.

3.6 Program Increment Planning

If applicable to the Call order, the vendor shall secure appropriate space for program increment planning sessions and other meetings requiring attendance by large groups of vendor personnel. The meeting space and travel by vendor personnel shall be included in the vendor's total firm fixed price (not expensed via ODCs). A separate travel line item or accounting can be requested at the call order level if needed.

If available, suitable and in the government's best interest, a facility owned or leased by the government may be used at no additional cost or requirement for reimbursement from the vendor.

If federal employees are requested to attend the meeting the vendor shall work with the COR and CO prior to finalizing the location and facilities to consider factors such as: the government's local presence, required federal employee travel funds availability, public perception and ethics regulations federal employees are subject to including, but not limited to, food, beverages and gifts. The vendor shall work with the COR and CO to complete required requests and reports to fulfill USDA's conference transparency, accountability and tracking requirements.

3.7 Contract Clauses and FPAC Information Technology Clauses

The USDA Contract Clauses automatically flow to all BPA call orders under this BPA. FPAC Special IT Clauses, Attachment B automatically flow to all BPA call orders.

3.8 Local Contracting Officer Representative

Unless otherwise identified, there will be one single COR for the BPA and call orders. In the event an order is issued at an agency other than FPAC, a local COR should be identified.

4.0 BPA ATTACHMENTS LIST

Attachment A – Removed

Attachment B – FPAC Special IT Clauses

Attachment C – System Development Lifecycle Document (SDLC)

Attachment D – Removed

BPA Price List 12314420A0034 Deloitte		Year 1 - 2020-2021			Year 2 - 2021-2022			Year 3 - 2022-2023			Year 4 - 2023-2024			Year 5 - 2024-2025		
Labor Category Role	**GSA Schedule 70 Labor Category**	**GSA Schedule 70 Hourly Rate**	**BPA Discount %**	**BPA Discounted Hourly Rate**	**GSA Schedule 70 Hourly Rate**	**BPA Discount %**	**BPA Discounted Hourly Rate**	**GSA Schedule 70 Hourly Rate**	**BPA Discount %**	**BPA Discounted Hourly Rate**	**GSA Schedule 70 Hourly Rate**	**BPA Discount %**	**BPA Discounted Hourly Rate**	**GSA Schedule 70 Hourly Rate**	**BPA Discount %**	**BPA Discounted Hourly Rate**
Automated Test Architect	(54151S) IT Sr. Consultant	$185.22	6.00%	$174.11	$185.22	3.27%	$179.16	$185.22	0.46%	$184.36	$185.22	0.00%	$185.22	$185.22	0.00%	$185.22
Configuration Specialist	(54151S) IT Project Delivery Manager	$144.73	5.00%	$137.49	$144.73	2.25%	$141.48	$144.73	0.00%	$144.73	$144.73	0.00%	$144.73	$144.73	0.00%	$144.73
Configurator I	(54151S) Project Controller II	$85.70	4.99%	$81.42	$85.70	2.24%	$83.78	$85.70	0.00%	$85.70	$85.70	0.00%	$85.70	$85.70	0.00%	$85.70
Configurator II	(54151S) Project Controller III	$114.40	5.00%	$108.68	$114.40	2.25%	$111.83	$114.40	0.00%	$114.40	$114.40	0.00%	$114.40	$114.40	0.00%	$114.40
Configurator III	(54151S) IT Center Associate Lead	$133.77	9.00%	$121.73	$133.77	6.36%	$125.26	$133.77	3.65%	$128.89	$133.77	0.85%	$132.63	$133.77	0.00%	$133.77
Developer I	(54151S) IT Analyst	$129.66	3.00%	$125.77	$129.66	0.19%	$129.42	$129.66	0.00%	$129.66	$129.66	0.00%	$129.66	$129.66	0.00%	$129.66
Developer II	(54151S) IT Consultant	$149.05	4.00%	$143.09	$149.05	1.21%	$147.24	$149.05	0.00%	$149.05	$149.05	0.00%	$149.05	$149.05	0.00%	$149.05
Developer III	(54151S) IT Sr. Consultant	$185.22	6.00%	$174.11	$185.22	3.27%	$179.16	$185.22	0.46%	$184.36	$185.22	0.00%	$185.22	$185.22	0.00%	$185.22
DevOps Engineer I	(54151S) IT Consultant	$149.05	4.00%	$143.09	$149.05	1.21%	$147.24	$149.05	0.00%	$149.05	$149.05	0.00%	$149.05	$149.05	0.00%	$149.05
DevOps Engineer II	(54151S) IT Sr. Consultant	$185.22	6.00%	$174.11	$185.22	3.27%	$179.16	$185.22	0.46%	$184.36	$185.22	0.00%	$185.22	$185.22	0.00%	$185.22
Functional Lead	(54151S) IT Sr. Consultant	$185.22	6.00%	$174.11	$185.22	3.27%	$179.16	$185.22	0.46%	$184.36	$185.22	0.00%	$185.22	$185.22	0.00%	$185.22
GIS/Geospatial/Esri Architect	(54151S) IT Sr. Manager	$267.12	18.00%	$219.04	$267.12	15.62%	$225.39	$267.12	13.17%	$231.93	$267.12	10.65%	$238.66	$267.12	8.06%	$245.58
GIS/Geospatial/Esri Developer	(54151S) IT Sr. Consultant	$185.22	6.00%	$174.11	$185.22	3.27%	$179.16	$185.22	0.46%	$184.36	$185.22	0.00%	$185.22	$185.22	0.00%	$185.22
Interactive Experience Designer	(54151S) IT Sr. Consultant	$185.22	6.00%	$174.11	$185.22	3.27%	$179.16	$185.22	0.46%	$184.36	$185.22	0.00%	$185.22	$185.22	0.00%	$185.22
Interface Specialist	(54151S) IT Analyst	$129.66	3.00%	$125.77	$129.66	0.19%	$129.42	$129.66	0.00%	$129.66	$129.66	0.00%	$129.66	$129.66	0.00%	$129.66
MuleSoft Architect	(54151S) IT Sr. Manager	$267.12	18.00%	$219.04	$267.12	15.62%	$225.39	$267.12	13.17%	$231.93	$267.12	10.65%	$238.66	$267.12	8.06%	$245.58
MuleSoft Developer	(54151S) IT Consultant	$149.05	4.00%	$143.09	$149.05	1.21%	$147.24	$149.05	0.00%	$149.05	$149.05	0.00%	$149.05	$149.05	0.00%	$149.05
Product Manager	(54151S) IT Sr. Consultant	$185.22	6.00%	$174.11	$185.22	3.27%	$179.16	$185.22	0.46%	$184.36	$185.22	0.00%	$185.22	$185.22	0.00%	$185.22
Program Manager	(54151S) IT Partner/Principal/Director	$290.35	18.00%	$238.09	$290.35	15.62%	$244.99	$290.35	13.18%	$252.09	$290.35	10.66%	$259.40	$290.35	8.07%	$266.92
Project Manager	(54151S) IT Manager	$240.79	18.00%	$197.45	$240.79	15.62%	$203.18	$240.79	13.17%	$209.07	$240.79	10.66%	$215.13	$240.79	8.07%	$221.37
Project Specialist I	(54151S) IT Analyst	$129.66	3.00%	$125.77	$129.66	0.19%	$129.42	$129.66	0.00%	$129.66	$129.66	0.00%	$129.66	$129.66	0.00%	$129.66
Project Specialist II	(54151S) IT Consultant	$149.05	4.00%	$143.09	$149.05	1.21%	$147.24	$149.05	0.00%	$149.05	$149.05	0.00%	$149.05	$149.05	0.00%	$149.05
Project Specialist III	(54151S) IT Sr. Consultant	$185.22	6.00%	$174.11	$185.22	3.27%	$179.16	$185.22	0.46%	$184.36	$185.22	0.00%	$185.22	$185.22	0.00%	$185.22
Project Specialist IV	(54151S) IT Manager	$240.79	18.00%	$197.45	$240.79	15.62%	$203.18	$240.79	13.17%	$209.07	$240.79	10.66%	$215.13	$240.79	8.07%	$221.37
Project Support I	(54151S) Project Controller III	$114.40	5.00%	$108.68	$114.40	2.25%	$111.83	$114.40	0.00%	$114.40	$114.40	0.00%	$114.40	$114.40	0.00%	$114.40
Project Support II	(54151S) IT Center Associate Lead	$133.77	9.00%	$121.73	$133.77	6.36%	$125.26	$133.77	3.65%	$128.89	$133.77	0.85%	$132.63	$133.77	0.00%	$133.77
Project Support III	(54151S) IT Project Delivery Manager	$144.73	5.00%	$137.49	$144.73	2.25%	$141.48	$144.73	0.00%	$144.73	$144.73	0.00%	$144.73	$144.73	0.00%	$144.73
Project Support IV	(54151S) IT Project Delivery Manager II	$171.41	5.00%	$162.84	$171.41	2.25%	$167.56	$171.41	0.00%	$171.41	$171.41	0.00%	$171.41	$171.41	0.00%	$171.41
QA Specialist	(54151S) IT Center Associate Lead	$133.77	9.00%	$121.73	$133.77	6.36%	$125.26	$133.77	3.65%	$128.89	$133.77	0.85%	$132.63	$133.77	0.00%	$133.77
Regression Tester	(54151S) IT Center Associate Lead	$133.77	9.00%	$121.73	$133.77	6.36%	$125.26	$133.77	3.65%	$128.89	$133.77	0.85%	$132.63	$133.77	0.00%	$133.77
Release Train Engineer I	(54151S) IT Manager	$240.79	18.00%	$197.45	$240.79	15.62%	$203.18	$240.79	13.17%	$209.07	$240.79	10.66%	$215.13	$240.79	8.07%	$221.37
Release Train Engineer II	(54151S) IT Sr. Manager	$267.12	18.00%	$219.04	$267.12	15.62%	$225.39	$267.12	13.17%	$231.93	$267.12	10.65%	$238.66	$267.12	8.06%	$245.58
Salesforce Certified Technical Architect/SME	(54151S) IT Sr. Manager	$267.12	18.00%	$219.04	$267.12	15.62%	$225.39	$267.12	13.17%	$231.93	$267.12	10.65%	$238.66	$267.12	8.06%	$245.58
Salesforce Developer	(54151S) IT Consultant	$149.05	4.00%	$143.09	$149.05	1.21%	$147.24	$149.05	0.00%	$149.05	$149.05	0.00%	$149.05	$149.05	0.00%	$149.05
Scrum Master	(54151S) IT Manager	$240.79	18.00%	$197.45	$240.79	15.62%	$203.18	$240.79	13.17%	$209.07	$240.79	10.66%	$215.13	$240.79	8.07%	$221.37
Scrum Master / PO Liaison	(54151S) IT Manager	$240.79	18.00%	$197.45	$240.79	15.62%	$203.18	$240.79	13.17%	$209.07	$240.79	10.66%	$215.13	$240.79	8.07%	$221.37
Solutions Train Engineer/SAFe SME	(54151S) IT Sr. Manager	$267.12	18.00%	$219.04	$267.12	15.62%	$225.39	$267.12	13.17%	$231.93	$267.12	10.65%	$238.66	$267.12	8.06%	$245.58
Technical Architect - Salesforce	(54151S) IT Manager	$240.79	18.00%	$197.45	$240.79	15.62%	$203.18	$240.79	13.17%	$209.07	$240.79	10.66%	$215.13	$240.79	8.07%	$221.37
Visual Designer	(54151S) IT Consultant	$149.05	4.00%	$143.09	$149.05	1.21%	$147.24	$149.05	0.00%	$149.05	$149.05	0.00%	$149.05	$149.05	0.00%	$149.05

Offerors may add labor category roles as needed to best reflect those that may be required by the BPA and potential call orders. Offerors must annotate any additions to this table. Offerors are not required to add any additional labor categories.

USDA CONTRACT CLAUSES

**ALL APPLICABLE GSA FEDERAL SUPPLY SCHEDULE CLAUSES AUTOMATICALLY FLOW TO THIS SOLICITATION AND RESULTING AWARD(S).*

1. **52.203-16 PREVENTING PERSONAL CONFLICTS OF INTEREST (JUN 2020)**

2. **52.204-9 PERSONAL IDENTITY VERIFICATION OF CONTRACTOR PERSONNEL (JAN 2011)**

3. **52.204-13 SYSTEM FOR AWARD MANAGEMENT MAINTENANCE (OCT 2018)**

4. **52.204-18 COMMERCIAL AND GOVERNMENT ENTITY CODE MAINTENANCE (AUG 2020)**

5. **52.204-21 BASIC SAFEGUARDING OF COVERED CONTRACTOR INFORATION SYSTEMS (JUN 2016)**

(a) Definitions. As used in this clause–

"Covered contractor information system" means an information system that is owned or operated by a contractor that processes, stores, or transmits Federal contract information.

"Federal contract information" means information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government, but not including information provided by the Government to the public (such as on public websites) or simple transactional information, such as necessary to process payments.

"Information" means any communication or representation of knowledge such as facts, data, or opinions, in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual (Committee on National Security Systems Instruction (CNSSI) 4009).

"Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information (44 U.S.C. 3502).

"Safeguarding" means measures or controls that are prescribed to protect information systems.

(b) Safeguarding requirements and procedures.

(1) The Contractor shall apply the following basic safeguarding requirements and procedures to protect covered contractor information systems. Requirements and procedures for basic safeguarding of covered contractor information systems shall include, at a minimum, the following security controls:

(i) Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).

(ii) Limit information system access to the types of transactions and functions that authorized users are permitted to execute.

(iii) Verify and control/limit connections to and use of external information systems.

(iv) Control information posted or processed on publicly accessible information systems.

(v) Identify information system users, processes acting on behalf of users, or devices.

(vi) Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.

(vii) Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse.

(viii) Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.

(ix) Escort visitors and monitor visitor activity; maintain audit logs of physical access; and control and manage physical access devices.

(x) Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.

(xi) Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.

(xii) Identify, report, and correct information and information system flaws in a timely manner.

(xiii) Provide protection from malicious code at appropriate locations within organizational information systems.

(xiv) Update malicious code protection mechanisms when new releases are available.

(xv) Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.

(2) Other requirements. This clause does not relieve the Contractor of any other specific safeguarding requirements specified by Federal agencies and departments relating to covered contractor information systems generally or other Federal safeguarding requirements for controlled unclassified information (CUI) as established by Executive Order 13556.

(c) Subcontracts. The Contractor shall include the substance of this clause, including this paragraph (c), in subcontracts under this contract (including subcontracts for the acquisition of commercial items, other than commercially available off-the-shelf items), in which the subcontractor may have Federal contract information residing in or transiting through its information system.

(End of Clause)

6. **52.204-25 PROHIBITION ON CONTRACTING FOR CERTAIN TELECOMMUNICATIONS AND VIDEO SURVEILLANCE SERVICES OR EQUIPMENT (AUG 2020).**

7. **52.242-15 STOP WORK ORDER (AUG 1989)**

8. **52.245-1 GOVERNMENT PROPERTY (JAN 2017)**

9. **52.252-2 CLAUSES INCORPORATED BY REFERENCE (FEB 1998)**

This contract incorporates one or more clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. Also, the full text of a clause may be accessed electronically at this/these address(es): http://www.acquisition.gov/far

(End of clause)

10. **AGAR 452.224-70 CONFIDENTIALITY OF INFORMATION (FEB 1988)**

(a) Confidential information, as used in this clause, means --

(1) information or data of a personal nature, proprietary about an individual, or

(2) information or data submitted by or pertaining to an organization.

(b) In addition to the types of confidential information described in (a)(1) and (2) above, information which might require special consideration with regard to the timing of its disclosure may derive from

studies or research, during which public disclosure of primarily invalidated findings could create an erroneous conclusion which might threaten public health or safety if acted upon.

(c) The Contracting Officer and the Contractor may, by mutual consent, identify elsewhere in this contract specific information and/or categories of information which the Government will furnish to the Contractor or that the Contractor is expected to generate which is confidential. Similarly, the contracting Officer and the Contractor may, by mutual consent, identify such confidential information from time to time during the performance of the contract. Failure to agree will be settled pursuant to the "Disputes" clause.

(d) If it is established that information to be utilized under this contract is subject to the Privacy Act, the Contractor will follow the rules and procedures of disclosure set forth in the Privacy Act of 1974, 5 U.S.C. 552a, and implementing regulations and policies, with respect to systems of records determined to be subject to the Privacy Act.

(e) Confidential information, as defined in (a)(1) and (2) above, shall not be disclosed without the prior written consent of the individual, institution or organization.

(f) Written advance notice of at least 45 days will be provided to the Contracting Officer of the Contractor's intent to release findings of studies or research, which have the possibility of adverse effects on the public or the Federal agency, as described in (b) above. If the Contracting Officer does not pose any objections in writing within the 45-day period, the contractor may proceed with disclosure. Disagreements not resolved by the Contractor and Contracting Officer will be settled pursuant to the "Disputes" clause.

(g) Whenever the Contractor is uncertain with regard to the proper handling of material under the contract, or if the material in question is subject to the Privacy Act or is confidential information subject to the provisions of this clause, the Contractor shall obtain a written determination from the Contracting Officer prior to any release, disclosure, dissemination, or publication.

(h) The provisions of paragraph (e) of this clause shall not apply when the information is subject to conflicting or overlapping provisions in other Federal, State or local laws.

(End of Clause)

11. AGAR 452.237-74 KEY PERSONNEL (FEB 1988)

(a) The Contractor shall assign to this contract the following key personnel:

(b) During the first ninety (90) days of performance, the Contractor shall make no substitutions of key personnel unless the substitution is necessitated by illness, death, or termination of employment. The Contractor shall notify the Contracting Officer within 15 calendar days after the occurrence of any of these events and provide the information required by paragraph (c) below. After the initial 90-day period, the Contractor shall submit the information required by paragraph (c) to the Contracting Officer at least 15 days prior to making any permanent substitutions.

(c) The Contractor shall provide a detailed explanation of the circumstances necessitating the proposed substitutions, complete resumes for the proposed substitutes, and any additional information requested by the Contracting Officer. Proposed substitutes should have comparable qualifications to those of the persons being replaced. The Contracting Officer will notify the Contractor within 15 calendar days after receipt of all required information of the decision on substitutions. The contract will be modified to reflect any approved changes of key personnel.

(End of Clause)

12. AGAR 452.237-75 RESTRICTIONS AGAINST DISCLOSURE (FEB 1988)

(a) The Contractor agrees, in the performance of this contract, to keep all information contained in source documents or other media furnished by the Government in the strictest confidence. The Contractor also agrees not to publish or otherwise divulge such information in whole or in part in any manner or form, or to authorize or permit others to do so, taking such reasonable measures as are necessary to restrict access to such information while in the Contractor's possession, to those employees needing such information to perform the work provided herein, i.e., on a "need to know" basis. The Contractor agrees to immediately notify in writing, the Contracting Officer, named herein, in the event that the Contractor determines or has reason to suspect a breach of this requirement.

(b) The Contractor agrees not to disclose any information concerning the work under this contract to any persons or individual unless prior written approval is obtained from the Contracting Officer. The Contractor agrees to insert the substance of this clause in any consultant agreement or subcontract hereunder.

(End of Clause)

13. LOCAL CLAUSE – INVOICING PROCEDURES

(a) Invoices shall be submitted electronically through the Department of Treasury's Invoice Processing Platform (IPP). The contractor shall follow instructions on how to register and submit invoices via IPP as prescribed at the IPP website https://www.ipp.gov/.

(b) Additional Information regarding what constitutes a proper invoice can be found by reviewing the Prompt Payment Act (31 USC Chapter 32 - PROMPT PAYMENT ACT).

(c) A complete contractor-generated invoice shall be provided electronically (either as an attachment via IPP or via email direct to the ACO and COR) along with applicable back up documentation.

(d) The Contractor shall submit any other information or documentation required by other clauses of the contract/order to support the invoice request such as reports, copies of travel vouchers, hotel and meal receipts, supporting paid invoices, receiving/acceptance reports, etc. Original receipts shall be maintained by the Contractor and made available to Government auditors upon request.

(End of Clause)

FPAC SPECIAL IT CLAUSES

1.0 INFORMATION SECURITY

1.1. Information Security Incidents

An Information Security Incident is an incident that includes the known, potential, or suspected exposure, loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or unauthorized access of any Contractor or Government systems or information, including, but not limited to, Sensitive Information.

1.1.1. Information Security Incident Reporting Requirements

All Information Security Incidents must be reported in accordance with the requirements below, even if it is believed the Incident may be limited, small, or insignificant.

a) The Contractor must report all Information Security Incidents immediately, but not later than 30 minutes after becoming aware of the Incident.
b) Copy the Contracting Officer Representative (COR) if possible, or if Contracting Officer Representative (COR) email is not immediately available; contact the Contracting Officer Representative (COR) immediately after reporting the incident.
c) Do NOT include any Sensitive Information in the subject or body of any e-mail. To transmit Sensitive Information, use FIPS 140-2 compliant encryption methods to protect Sensitive Information in attachments to email. Passwords must **not** be communicated in the same email as the attachment.

1.1.2. Information Security Incident Response Requirements

a) All determinations related to Information Security Incidents, including response activities, notifications to affected individuals and/or Federal agencies, and related services (e.g., credit monitoring) will be made by authorized USDA officials.
b) The Contractor must provide full access and cooperation for all activities (determined by the authorized Government official to be required) to ensure an effective Incident Response, including providing all requested images, log files, and event information to facilitate rapid resolution of Information Security Incidents.
c) Incident Response activities determined to be required may include but are not limited to: inspections, investigations, forensic reviews, data analyses & processing, and final determinations of responsibility for the Incident and/or liability for any additional Response activities.
d) USDA, at its sole discretion, may obtain the assistance of Federal agencies and/or third party firms to aid in Incident Response activities.

1.2. Information Types

The term Information is synonymous with Data, regardless of format or medium. Personally Identifiable Information (PII) is a subset of Sensitive Information. Sensitive PII is a subset of PII, and therefore a subset of Sensitive Information. All requirements for Sensitive Information apply to PII and Sensitive PII. All requirements for PII apply to Sensitive PII.

1.2.1. Sensitive Information

Sensitive Information is any information, which if lost, compromised, or disclosed, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual, the Government, or the Government's interests. Sensitive Information is subject to stricter handling requirements because of the increased risk if the data is compromised. Some categories of Sensitive Information include Financial, Medical/Health, Legal, Strategic, Security, Intellectual Property & Business, Human Resources, Personally Identifiable Information (PII), and Sensitive PII. These categories of information require appropriate protection as stand-alone information and may require additional protection in aggregate.

1.2.2. Personally Identifiable Information (PII)

PII, as defined in OMB Memorandum M-07-16, refers to information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important to recognize that non-PII can become PII whenever additional information [that is publicly available] — in any medium and from any source — is or can be combined to identify an individual. As an example, PII includes a name and an address because it uniquely identifies an individual, but alone may not constitute Sensitive PII.

1.2.3. Sensitive PII

Sensitive PII refers to information that can be used to target, harm, or coerce an individual or entity, assume or alter an individual's or entity's identity, or alter the outcome of an individual's or entity's activities. Sensitive PII requires stricter handling because of the increased risk to an individual or associates if the information is compromised. Some categories of Sensitive PII include stand-alone information, such as Social Security numbers (SSN) or biometric identifiers. Other information such as a financial account, date of birth, maiden names, citizenship status, or medical information, in conjunction with the identity of an individual (directly or indirectly inferred), is also considered Sensitive PII. In addition, the context of the information may determine whether it is sensitive, such as a list of employees with poor performance ratings or a list of employees who have filed a grievance or complaint.

1.3. Compliance with Security IT Policies

Information systems and system services provided by the Contractor must comply with the current USDA IT security and privacy policies, specifically the 3500 – 3599 Cyber Security Department regulations - https://www.ocio.usda.gov/policy-directives-records-forms/directives-categories.

The Contractor is required to comply with current Federal regulations and guidance found in the Federal Information Security Modernization act of 2014 (FISMA); Privacy Act of 1974; E-Government Act of 2002, Section 208; National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) and the 800-Series Special Publications (SP), specifically 800-40, Guide to Enterprise Patch Management Technologies; Office of Management and Budget (OMB) memoranda; USDA Information Security Program policies and other relevant Federal laws and regulations with which USDA must comply.

House Resolution 83-15 "*Consolidated and Further Continuing Appropriations Act, 2015"* requires that USDA demonstrate each project/investment is "being managed in accordance with applicable lifecycle

management policies and guidance." This mandates that USDA development projects are required to follow the Agency's System Development Lifecycle (SDLC). All projects listed in Farm Service Agency Farm Programs IT plan for expenditure can expect to be audited for compliance. Audits may occur at any time after the plan for expenditure is submitted to Congress.

The Contractor must protect information regarding security issues and associated documentation to limit the likelihood that vulnerabilities in operational client software are exposed. If new vulnerabilities are identified after the acceptance of COTS software, the vendor must review and remediate the vulnerabilities and present the results for Government approval within the timeframes documented in USDA IT security policies.

1.4. Security Assessment and Authorization

a. This contract requires the Contractor to develop, deploy, and/or use information systems to access and/or store Government information, including Sensitive Information. The Contractor must cooperate and support the Government in the development of required documentation and artifacts.
b. All information systems that input, store, process, and/or output Government information must be provided an Authority to Operate (ATO) signed by the authorizing official as identified by the CIO. The Contractor must adhere to current policies, procedures, and guidance for security Assessment and Authorization (A&A) activities.

1.5. Federal Reporting Requirements

Contractors operating information systems must comply with Federal Information Security Modernization Act (FISMA) reporting requirements. Annual and quarterly data collection will be coordinated by the Government. Contractors must provide the Government with the requested information based on the timeframes provided with each request. Reporting requirements are determined by the Office of Management and Budget (OMB), and may change each reporting period. The Contractor will provide the Government with all information to fully satisfy FISMA reporting requirements for Contractor systems.

1.6. Acquiring And/Or Implementing Software Applications

Secure Coding Skills: Contractor must certify that at least one member of each programming team working on any code (including C, Java, .Net, ASP.NET, Visual Basic) to be delivered to the Govt. has earned the Global Information Assurance Certification for Secured Software Programming or equivalent.
Source code testing, binary code testing, application scanning, and penetration testing: At least one (1) week prior to delivery of any code due under this contract, Contractor will deliver to the COR the following reports covering all code that will be delivered:
A. Source code testing results showing all potential security flaws identified by at least one of the commercial source code testing tools approved by the Office of the Chief Information Officer of USDA. On the report, the Contractor will highlight all vulnerabilities rated "critical" and "high." The Contractor must then correct the vulnerabilities, resend the code, and ensure the health of delivered source code.
B. For web applications, web application scanning test results showing all potential security flaws identified by at least one of the commercial web application scanning tools approved by the Office of the Chief Information Officer of USDA. On the report, the Contractor will highlight all vulnerabilities rated "critical" and "high."
C. For all applications: application penetration results.

Copyright Management and Responsibility: By delivering applications or programming code to the Federal Government, the vendor or Contractor certifies that they have the proper authority to transfer the property and will defend the Government against copyright or other lawsuit resulting from the application or programming delivered.

1.7. Processing, Storing, Transmitting Government Data to Non-Government System

The Contractor or other external organizations will develop, provide, implement, and maintain an IT System Security Plan for any system that includes acquisition, transmission or analysis of data owned by the Government with significant replacement cost should the Contractor's and other external organization's copy be corrupted. This plan will describe the processes and procedures that will be followed to ensure appropriate security of IT resources that are developed, processed, or used under this contract. The plan will describe those parts of the contract to which this clause applies. The Contractor or other external organization's IT System Security Plan will be compliant with applicable Federal laws that include, but are not limited to: (e.g., the Clinger-Cohen Act of 1996 and the Federal Information Security Management Act of 2002). The IT System Security Plan will meet IT security requirements in accordance with Government policies and procedures that include, but are not limited to: National Institute of Standards and Technology (NIST) SP 800-53 Guidelines.
The Contractor and other external organizations will ensure that the appropriate security banners are displayed on all Government systems (both public and private) operated by the contractors and other external organizations prior to allowing anyone access to the system.

2.0 PERSONNEL

2.1. Personnel Security

2.1.1. Background Investigation Requirements

Contractor personnel must be able to obtain a favorable suitability decision in accordance with 5 CFR part 731.

The duties of this contract range from low risk to high risk positions and, as such, Contractor personnel will be required to submit all required documentation necessary for the agency to provide a favorable preliminary decision on suitability. This decision is required prior to commencing work on the contract.

Contractor personnel who receive an unfavorable suitability decision must be immediately removed from consideration for work on the contract.

The company is accountable for selecting personnel capable of receiving favorable suitability determinations; consequences for advancing personnel not able to pass government background checks may include providing invoice credits effectively reimbursing the government for background check expenses. Performance delays or detrimental project outcomes due to not onboarding or removal of staff will be directly attributable to the vendor and documented.

2.1.2. HSPD-12 -Credentials

Contractor personnel must complete necessary requirements to obtain HSPD-12 credentials immediately upon beginning work on the contract. Failure to obtain HSPD-12 credentials is grounds for removal/suspension of Contractor personnel from the contract.

2.2. Training

2.2.1. Mandatory Government Training

Mandatory training must be completed by the required dates by all contract employees. Mandatory Government training classes may be completed during work hours. It is the intent of USDA to provide thirty (30) calendar days written notice of annual training requirements to the Contractor. In the event the Contractor does not receive thirty (30) calendar day notice, the Contractor is still required to complete the training by the specified required date(s).

These mandatory courses are typically provided through USDA's education/learning application and are free-of-charge. The education/learning application will typically load mandatory training to the individual's education/learning application profile to-do list. The COR will notify the Contractor of new training requirements. Training can typically be completed within 30-60 minutes. This training includes:

- Information Security Awareness Training (ISAT) - All Contractor personnel working on this contract are required to complete USDA provided ISAT both before beginning work and annually thereafter. Failure to take this training within the prescribed window will result in removal of the Contractor employee from the contract.
- Records Management training - is a one-time training that is required for everyone within ninety (90) days of their start date.
- Other training that is federally mandated or required by the agency.

3.0 SECTION 508 – ACCESSIBILITY OF INFORMATION AND COMMUNICATIONS TECHNOLOGY

(a) This Statement of Work (SOW) is subject to Section 508 of the Rehabilitation Act of 1973 (29 U.S.C. 794d) as amended by the Workforce Investment Act of 1998 (P.L. 105-220). Specifically, subsection 508(a)(1) requires that when the Federal Government procures Information and Communications Technology (ICT)[1], the ICT must allow Federal employees and members of the public with disabilities comparable access to and use of information and data provided to Federal employees and members of the public without disabilities.
(b) The ICT accessibility standards as 36 CFR Part 1194 were developed by the Architectural and Transportation Barriers Compliance Board (also known as the Access Board) and apply to contracts, task orders, and indefinite quantity contracts on or after June 25, 2001.
(c) Each Information and Communications Technology (ICT) product or service furnished under this contract shall comply with the Information and Communications Technology Accessibility Standards (36 CFR 1194), as specified in the contract, at a minimum. If the Contracting Officer determines any furnished product or service is not in compliance with the contract, the Contracting Officer will promptly inform the Contractor in writing. The Contractor shall, without charge to the Government, repair or replace the non-compliant products or services within a period of time specified by the

[1] Please note that the term Information and Communications Technology (ICT) is synonymous with Electronic and Information Technology (EIT), the previously used term. The term ICT will be used to meet international standards after the release of the Section 508 Refresh.

Government in writing. If such repair or replacement is not completed within the time specified, the Government shall have the following recourses:

1) Cancellation of the contract, delivery, or task order, purchase or line item without termination liabilities; or
2) In the case of custom Information and Communications Technology (ICT) being developed by a contractor for the Government, the Government shall have the right to have any necessary changes made or repairs performed by itself or by another firm for the non-compliant ICT, with the contractor liable for reimbursement to the Government for any expenses incurred thereby.

(d) The contractor must ensure that all ICT products and services that are less than fully compliant with the accessibility standards are provided pursuant to extensive market research and are the most current compliant products or services available to satisfy the contract requirements.
(e) For every ICT product or service accepted under this contract by the Government that does not comply with 36 CFR 1194, the contractor shall, at the discretion of the Government, make every effort to replace or upgrade it with a compliant equivalent product or service, if commercially available and cost neutral, on either a contract specified refresh cycle for the product or service, or on a contract effective option/renewal date, whichever shall occur first.

3.1. Section 508 Compliance

The software shall comply with the standards, policies, and procedures below. In the event of conflicts between the referenced documents and this SOW, the SOW shall take precedence.

Section 508 Accessibility Standards

1) 29 U.S.C. 794d (Rehabilitation Act as amended)
2) 36 CFR 1194 (Section 508 standards)
3) http://www.access-board.gov/sec508/508standards.htm (Section 508 standards)
4) FAR 39.2 (Section 508)
5) http://www.ocio.usda.gov/document/departmental-regulation-4030-001 (USDA standards, policies, and procedures for Section 508)

In addition, all contract deliverables are subject to these standards.
All web content or communications materials produced, regardless of format (text, audio, video, etc.), must conform to the applicable Section 508 standards to allow Federal employees and members of the public with disabilities comparable access to and use of information and data provided to Federal employees and members of the public without disabilities. All contractors (including sub-contractors) and consultants responsible for preparing or posting content must comply with the applicable Section 508 accessibility standards and, where applicable, those set forth in the referenced policy or standards document above. Remediation of any materials that do not comply with the applicable provisions of 36 CFR Part 1194 as set forth in the SOW shall be the responsibility of the contractor or consultant.

The following Section 508 provisions apply to the products and/or services identified in this SOW:

- 36 CFR Part 1194.21 provisions a-l
- 36 CFR Part 1194.22 provisions a-p
- 36 CFR Part 1194.23 provisions a-k[4]
- 36 CFR Part 1194.24 provisions a-e
- 36 CFR Part 1194.25 provisions a-j[4]
- 36 CFR Part 1194.26 provisions a-d
- 36 CFR Part 1194.31 provisions a-f
- 36 CFR Part 1194.41 provisions a-c

The following Section 508 provisions apply for software development material identified in this SOW:

For **software development, software applications, and operating systems** the Vendor shall comply with the following standards, policies, and procedures:
Section 508 Accessibility Standards

1) 29 U.S.C. 794d (Rehabilitation Act as amended)
2) 36 CFR 1194 (Section 508 standards)
    a. 36 CFR Part 1194.21 provisions a-l
    b. 36 CFR Part 1194.31 provisions a-f
    c. 36 CFR Part 1194.41 provisions a-c

For **web-based applications** (intranet, internet information and applications, 16 rules), the Vendor shall comply with the following standards, policies, and procedures:
Section 508 Accessibility Standards

1) 29 U.S.C. 794d (Rehabilitation Act as amended)
2) 36 CFR 1194 (Section 508 standards)
    a. 36 CFR Part 1194.21 provisions a-l
    b. 36 CFR Part 1194.22 provisions a-p
    c. 36 CFR Part 1194.31 provisions a-f
    d. 36 CFR Part 1194.41 provisions a-c

For **telecommunication** products and services, the *Vendor* shall comply with the following standards, policies, and procedures:
Section 508 Accessibility Standards

1) 29 U.S.C. 794d (Rehabilitation Act as amended)
2) 36 CFR 1194 (Section 508 standards)
    a. 36 CFR Part 1194.23 provisions a-k
    b. 36 CFR Part 1194.31 provisions a-f
    c. 36 CFR Part 1194.41 provisions a-c

For **video and multimedia applications** (including training materials), the Vendor shall comply with the following standards, policies, and procedures:
Section 508 Accessibility Standards

1) 29 U.S.C. 794d (Rehabilitation Act as amended)
2) 36 CFR 1194 (Section 508 standards)
    a. 36 CFR Part 1194.24 provisions a-e
    b. 36 CFR Part 1194.31 provisions a-f
    c. 36 CFR Part 1194.41 provisions a-c

For **self-contained and closed products**, the Vendor shall comply with the following standards, policies, and procedures:
Section 508 Accessibility Standards

1) 29 U.S.C. 794d (Rehabilitation Act as amended)
2) 36 CFR 1194 (Section 508 standards)
    a. 36 CFR Part 1194.21 provisions a-l
    b. 36 CFR Part 1194.25 provisions a-j
    c. 36 CFR Part 1194.31 provisions a-f

d. 36 CFR Part 1194.41 provisions a-c

For **desktop and portable computers**, the Vendor shall comply with the following standards, policies, and procedures:
Section 508 Accessibility Standards

1) 29 U.S.C. 794d (Rehabilitation Act as amended)
2) 36 CFR 1194 (Section 508 standards)
   a. 36 CFR Part 1194.21 provisions a-l
   b. 36 CFR Part 1194.26 provisions a-d
   c. 36 CFR Part 1194.31 provisions a-f
   d. 36 CFR Part 1194.41 provisions a-c

For **help desk and other support services**, the Vendor shall comply with the following standards, policies, and procedures:
Section 508 Accessibility Standards

1) 29 U.S.C. 794d (Rehabilitation Act as amended)
2) 36 CFR 1194 (Section 508 standards)
   a. 36 CFR Part 1194.31 provisions a-f
   b. 36 CFR Part 1194.41 provisions a-c

If the help desk or other support services include **training**, Vendor must also comply with the following standards, policies, and procedures in addition to 36 CFR Part 1194.31 provisions a-f and 36 CFR Part 1194.41 provisions a-c:

a. 36 CFR Part 1194.21 provisions a-l (installable and web-based training)
b. 36 CFR Part 1194.22 provisions a-p (web-based software)

All Information and Communications Technology (ICT) subject to the 36 CFR 1194 standards will have a Section 508 usability and acceptance test where Section 508 compliance will be validated. This test must be administered by a Federal Section 508 Testing Center.
All maintenance for Information and Communications Technology that requires upgrades, modifications, installations, and purchases will adhere to the Section 508 standards and 36 CFR 1194.

3.2. WCAG 2.0 Compliance

The software shall comply with the standards, policies, and procedures below. In the event of conflicts between the referenced documents and this SOW, the SOW shall take precedence.

Custom ICT Development Services
When Vendor provides custom ICT development services pursuant to this contract, Vendor shall ensure the ICT fully conforms to the applicable Revised 508 Standards prior to delivery and before final acceptance.

Installation, Configuration, and Integration Services
When Vendor provides installation, configuration, or integration services for equipment and software pursuant to this contract, the offeror shall not install, configure, or integrate the equipment and software in a way that reduces the level of conformance with the applicable Revised 508 standards.

Maintenance, Upgrades, and Replacements
Vendor shall ensure maintenance upgrades, substitutions, and replacements to equipment and software pursuant to this contract do not reduce the original level of conformance with the applicable Revised 508 standards at the time of the contract award.

Service Personnel
Vendor shall ensure the personnel providing the labor hours possess the knowledge, skills, and ability necessary to address the applicable Revised 508 standards defined in this contract and shall provide supporting documentation upon request.

Hosting Services
When providing hosting services for electronic content provided by the agency, Vendor shall not implement the hosting services in a manner that reduces the existing level of conformance of the electronic content with applicable Revised 508 standards. Throughout the life of the contract, the agency reserves the right to perform testing on a vendor or contractor's hosted solution to verify conformance with this requirement.

Validation for ICT Items
When purchasing ICT where 1) 508 validation is not possible prior to award, 2) when ICT will be changed after the award, or 3) ICT will be hosted in a third-party environment, Vendor shall test and validate the ICT solution for conformance to the Revised 508 standards, in accordance with the requirement testing methods, as defined by the agency. Throughout the life of the contract, the agency reserves the right to perform testing to verify conformance with this requirement.

Documentation
Vendor shall maintain and retain full documentation of the measures taken to ensure compliance with the applicable requirements, including records of any testing or demonstrations conducted.

Conformance Reporting
Prior to acceptance, Vendor shall provide an Accessibility Conformance Report (ACR) for each ICT item that is developed, updated, configured for the agency, and when product substitutions are offered. The ACR should be based on the latest version of the Voluntary Product Accessibility Template (VPAT) provided by the Information Technology Industry Council (ITI). To be considered for award, an ACR must be submitted for each ICT item, and must be completed according to the instructions provided by ITI.

When the contractor is required to perform testing to validate conformance to the agency's accessibility requirements, Vendor shall provide a Supplemental Accessibility Conformance Report (SAR) that contains the following information:

- Accessibility test results based on the required test methods.
- Documentation of features provided to help achieve accessibility and usability for people with disabilities.
- Documentation of core functions that cannot be accessed by persons with disabilities.
- Documentation on how to configure and install the ICT item to support accessibility.
- When an ICT item is an authoring tool that generates content (including documents, reports, videos, multimedia productions, web content, etc.)., provide information on how the ICT item enables the creation of accessible electronic content that conforms to the Revised 508 Standards, including the range of accessible user interface elements the tool can create.

- Before final acceptance, the contractor shall provide a fully working demonstration of the completed ICT Item to demonstrate conformance to the agency's accessibility requirements. The demonstration shall expose where such conformance is and is not achieved.

Before acceptance, the agency reserves the right to perform independent testing to validate that the ICT solution provided by the contractor conforms to the applicable Revised 508 standards.

Non-Compliance
Before final acceptance of any ICT item, including updates and replacements, if Vendor claims its products or services satisfy the applicable Revised 508 standards specified in the contract vehicle, and the contracting officer determines that any furnished ICT item is not in compliance with such requirements, the contracting officer will promptly inform Vendor in writing of the non-compliance. Vendor shall, at no cost to the agency, repair or replace the non-compliant products or services within the period specified by the contracting officer.

4.0 COMPLIANCE WITH INTERNET PROTOCOL VERSION 6 (IPV6) IN ACQUIRING INFORMATION TECHNOLOGY

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.

5.0 DATA OWNERSHIP

5.1. Data and Deliverable Rights

All information such as software, data, designs, test materials, documents, documentation, notes, records, software tools acquired, and/or software source code and modifications produced by the Contractor under this contract is the sole property of the U.S. Government, which has unlimited rights to all materials and can determine the scope of publication and distribution. The Government retains ownership of all proprietary information and intellectual property generated under this contract.

5.2. Transfer of Ownership

All data and documentation, including all studies, reports, spreadsheets, software, data, designs, presentations, documentation, etc., produced by the Contractor or for the Government using this contract are the property of the Government upon its taking possession of task deliverables or upon termination of the contract.

6.0 NON-DISCLOSURE OF SENSITIVE OR PROPRIETARY INFORMATION

6.1. Non-Disclosure Agreement

Due to the sensitive nature of the data and information being worked with on a daily basis, all Contractor personnel assigned to the contract are required to complete the Government provided non-disclosure agreement prior to contract assignment to ensure information that is considered sensitive or proprietary is not compromised. Signed non-disclosure statements must be provided in accordance with the direction provided by the COR.

6.2. Data Access

The Contractor may be required to have access to live production data for the performance of this contract. Any records and data or information the Contractor may have access to may be highly sensitive and confidential. The Contractor must not divulge or misuse any information about files, data processing activities or functions, user IDs or passwords, or any other knowledge that may be gained, to anyone who is not authorized to have access to such information. It is the Contractor's responsibility to ensure that other persons have the proper authorization.

6.3. Privacy Act Compliance

Contractors must comply with the Privacy Act of 1974 requirements in the design, development, or operation of any system of records containing PII developed or operated for USDA or to accomplish an USDA function for a System of Records (SOR)

a. “System of Records” is defined as 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.

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

7.0 SOFTWARE LICENSE LINE ITEM DATA

In accordance with Office of Management and Budget Memorandum M-16-12, Category Management Policy 16-1: Improving the Acquisition and Management of Information Technology: Software Licensing, USDA must

maintain an inventory of its software licenses, including pricing data. The contractor shall provide line item pricing data on all software licenses provided to USDA at award and/or during performance of the contract/order. The attachment entitled "Software Template Line Item Pricing" must be completed and provided to the Contracting Officer's Representative within 10 days of award, or within 10 days of activation for licenses provided after the award date.

8.0 GOVERNMENT FURNISHED PROPERTY/INFORMATION/ACCESS

8.1. General

The Government must provide, without cost, the facilities, equipment, materials and services listed below. 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.

Contractor employees must clearly identify themselves as such at all times (badge display; identification announcement prior to or at the commencement of meetings and teleconferences; and correspondence including e-mail, etc.).

8.2. Contractor Access to IT Systems

a. Immediately following contract award, the Contractor must provide Contracting Officer's Representative a complete list of employee names, approval to work and current FY year completion certificate of USDA Information Security Awareness Training.
b. 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. Users of the systems will be subject to periodic auditing to ensure compliance with USDA and Agency policies.
c. Each Contractor is required to utilize Government furnished equipment as appropriate.
d. In coordination with the Contracting Officer Representative (COR), USDA may suspend or terminate the access to any systems and/or facilities when an Information Security Incident or other electronic access violation, use or misuse issue gives cause for such action. The suspension or termination may last until such time as USDA determines that the situation has been corrected or no longer exists.
e. Upon request of USDA, the Contractor must immediately return all Government issued equipment including, but not limited to Government issued external storage media (i.e. external drives, thumb drives).
f. Copying of USDA information outside of USDA controlled space or technology is prohibited. The Contractor must request permission from the COR to remove any data from the USDA environments. Upon request of USDA, the Contractor must immediately return all Government information and attest by non-disclosure agreement the Government information is properly and securely removed from media that is not Government furnished equipment.
g. The Contracting Officer's Representative (COR) must be notified at least five (5) days prior to a Contractor being removed from a contract. For unplanned terminations or removals of Contractors from the organization that occur with less than five (5) days' notice, the COR must be notified immediately. PIV cards issued to Contractors must be returned to the COR prior to departure.
h. All access to USDAIT systems will be accomplished using Personal Identity Verification (PIV) credentials, in accordance with NIST FIPS 201, Personal Identity Verification (PIV) of Federal Employees and Contractors. At USDA the PIV credential is branded "LincPass".

8.3. Property

8.3.1. Facilities

The Government will provide the Contractor access to buildings as required for meetings, planning or workshops, subject to the Contractor's employees obtaining the required clearances and approvals.

8.3.2. Safety

The Contractor must comply with all local safety regulations and procedures in effect at the respective installation locations.

8.3.3. Facilities and Equipment at Remote Work Locations
The Government will provide an imaged laptop for performance of this contract.

For work from a remote location, the Government will not reimburse the Contractor for costs associated with remote connectivity from cell phones, Wi-Fi access or Internet connection.

The Contractor must be responsible for ensuring the Contractor employee has an adequate and safe office space that sufficiently protects Government equipment and information from loss, theft or unauthorized access.

8.3.4. Materials
The Government must furnish basic reference manuals, and any revisions, updates, and changes thereto for use by the Contractor necessary to perform work assignments under the contract.

8.3.5. Validation of Government Furnished Items (GFI) and Equipment Inventory
The Contractor must develop and maintain a complete GFI inventory that must be made available to the Government upon request. Within three (3) work days of receipt of any GFI, the Contractor must validate the accuracy of the materials and notify the COR, in writing, of any discrepancies.

8.3.6. Use of Government Property
8.3.6.1. Office Equipment and Services
Office equipment and services in Government facilities include desk telephones, printers, copiers, multi-function devices, mail and postage services, Internet access, and electronic media. Office equipment also includes mobile/wireless telephones, hotspots, or smart devices, if authorized by the COR. Office equipment is to be used for official Government business only in the performance of the tasks in this contract.

8.3.6.2. Electronic Mail (E-mail)
All Government e-mail access and use by Contractor employees must be in support of the individual's official duties and task responsibilities. All information that is created, transmitted, received, obtained, or accessed in any way or captured electronically using USDA's e-mail systems is the property of the Government. Contractor employees must have clear identification in their e-mail signature block that identifies themselves as Contractor employees in support of USDA. Contractor employees are prohibited from forwarding e-mail generated from a Government provided e-mail account to personal mobile devices.

8.3.6.3. Security Violations Using Government Equipment
Any Contractor violating USDA security policies, guidelines, procedures, or requirements while using Government equipment or while accessing the USDA network may, without notice, will have their computer and network access terminated, be escorted from their work location, and have their physical access to their work location removed at the discretion of the CO/COR. The CO/COR will notify the Contractor of the security violation and request immediate removal of the contract employee.

8.3.6.4. Government Vehicles
The use of Government-furnished vehicles is NOT authorized under this contract.

8.3.7. Return of Government Property
All Government property, data, software, information, documentation and equipment whether furnished by the Government to the Contractor, created by the Contractor, or acquired by the Contractor with Government funding is property of the Government and must be delivered/transmitted to the COR upon termination or expiration of the call order or per instructions from the CO.

8.3.8. Conservation of Utilities While Working from a Government Facility
The Contractor must instruct employees in utilities conservation practices. The Contractor must be responsible for operating practices that preclude the waste of utilities, which must include:

§ Lights must be used only in areas where and when work is actually being performed.

§ Mechanical equipment controls for heating, ventilation, and air conditioning system must not be adjusted by the Contractor or by Contractor employees.
§ Water faucets or valves must be turned off after the required usage has been accomplished.

9.0 CONTRACT/CALL ORDER ADMINISTRATION

Contract Type: This will be a Blanket Purchase Agreement with firm fixed priced call order. Payment from USDA is based on the Contractor meeting the established milestones and agreed to tasks during the contracting phase. Projects under a Firm Fixed Price do not require tracking individual hours or costs against given level of effort hours.

Period of Performance: 15 September 2020 through 14 September 2025

Points of Contact: The contractor shall immediately bring problems or potential problems affecting performance to the attention of the Contracting Officer's Representative (COR). Verbal reports will be followed up with written reports when directed by the CO or COR. The following points of contact are to be used to communicate with the Government during the contract duration.

Contracting Officer's Representative (COR)
Michelle Jardine
801-844-2909
Michelle.jardine@usda.gov
Ste 6401, 125 S. State St
Salt Lake City, UT 84138

The Contracting Officer Representative (COR) may work with other Government personnel to monitor technical progress. The Contractor must 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.

Only the CO may take action 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.