Date

**Version X.x**

**NOTES TO THE AUTHOR/TEMPLATE INSTRUCTIONS**

This template includes instructions and boilerplate text. The author should note that:

* Each section provides instructions or describes the intent, assumptions, and context for content included in that section. Instructional text appears in *blue italicized text* throughout this template.
* Replace instructional text in each section with project specific information.
* Use or modify boilerplate examples of wording and formats for text and tables as appropriate.
* Search and replace all text enclosed in angle brackets - < > - with project specific information (e.g., <Project Name> or <Project Acronym>.

Follow these steps when using this template:

1. All documents must be compliant with Section 508 requirements. Refer to [FNS 504-508 Compliance Reference Library](https://fncspro.usda.net/offices/oit/Documents/Forms/AllItems.aspx?RootFolder=%2Foffices%2Foit%2FDocuments%2F504%2D508%20Compliance%20%2D%20Accessibility&View=%7BB47848DF%2D6059%2D4D43%2DAB0C%2D8ECEDC92AD4C%7D) or [Section508.gov](https://section508.gov/) for more information.
2. Modify any boilerplate text, as appropriate, for your specific project.
3. Use Styles for new sections such as Heading 1, Heading 2 and Std Para.
4. Place Table captions and descriptions *above* the table and centered. All tables must have an associated tag providing appropriate alternative text for Section 508 compliance.
5. Place Figure captions and descriptions *below* the figure and centered. All figures must have an associated tag providing appropriate alternative text for Section 508 compliance.
6. Update the Table of Contents and any List of Tables or List of Figures by right-clicking it and selecting Update field / Update entire table.
7. Delete this “Notes to the Author/Template Instructions” page and all instructional text to the author before finalizing the draft of the document.

**SDLC TEMPLATE REVISION HISTORY**

| **VERSION** | **DATE** | **AUTHOR** | **CHANGE DESCRIPTION** |
| --- | --- | --- | --- |
| 1.0 | 5/10/2019 | PMB | Created initial document |
| 2.1 | 10/18/2019 | PMB | 508 language and other updates |
| 2.2 | 11/02/2020 | Panum Group | Updated to reflect new FNS Agile SDLC processes and comply with Section 508 standards. |

**SDLC TEMPLATE CONTACT INFORMATION**

| **RESPONSIBILILTY** | **CONTACT PERSON** | **EMAIL ADDRESS** |
| --- | --- | --- |
| Portfolio Management Division Director, Chief Portfolio Officer | Joe Shaw | [Joseph.Shaw@usda.gov](mailto:Joseph.Shaw@usda.gov) |
| IT Governance Manager | Kevin Russ | [Kevin.Russ@usda.gov](mailto:Kevin.Russ@usda.gov) |
| SDLC Lead | Max Mounger | [Max.Mounger@usda.gov](mailto:Max.Mounger@usda.gov) |

**TABLE OF CONTENTS**

[1. PURPOSE 1](#_Toc52287908)

[2. BACKGROUND 1](#_Toc52287909)

[3. SCOPE 1](#_Toc52287910)

[3.1 Agile Development Methodology 1](#_Toc52287911)

[3.1.1 Backlog Management and Estimation 2](#_Toc52287912)

[3.1.2 Sprint 2](#_Toc52287913)

[3.1.3 Sprint Review/Demonstrations 2](#_Toc52287914)

[3.1.4 Metrics and Reporting 3](#_Toc52287915)

[3.2 Security 3](#_Toc52287916)

[3.3 Compliance with Applicable Laws, Regulations, and Standards 4](#_Toc52287917)

[3.4 General IT Security and Privacy Requirements 4](#_Toc52287918)

[3.5 Required Development Practices 5](#_Toc52287919)

[3.5.1 Standards 5](#_Toc52287920)

[3.5.2 Development Practices 5](#_Toc52287921)

[3.5.3 Security Practices 6](#_Toc52287922)

[3.5.4 Performance and Monitoring Practices 7](#_Toc52287923)

[3.5.5 Cloud Practices 8](#_Toc52287924)

[3.6 Quality Assurance and Configuration Management 8](#_Toc52287925)

[3.7 Data Rights 9](#_Toc52287926)

[4. PERFORMANCE AND TASKS 9](#_Toc52287927)

[4.1 Project Management Support 10](#_Toc52287928)

[4.1.1 Project Manager Support 10](#_Toc52287929)

[4.1.2 Contractor Responsibility with Project Documentation 11](#_Toc52287930)

[4.1.3 Decision Point Reviews 12](#_Toc52287931)

[4.1.4 Onboarding / Offboarding / Required Training 13](#_Toc52287932)

[4.1.5 Escalation 13](#_Toc52287933)

[4.2 System Development 13](#_Toc52287934)

[4.2.1 Requirements and Design 15](#_Toc52287935)

[4.2.2 Development and Testing 19](#_Toc52287936)

[4.2.3 Pre-Deployment 21](#_Toc52287937)

[4.2.4 Deployment 21](#_Toc52287938)

[4.3 Transition Support 22](#_Toc52287939)

[4.4 Miscellaneous Task Examples 22](#_Toc52287940)

[4.4.1 Sustainment 22](#_Toc52287941)

[4.4.2 System Monitoring and Support 25](#_Toc52287942)

[4.4.3 Data Mining 25](#_Toc52287943)

[4.4.4 Help Desk 26](#_Toc52287944)

[4.4.5 Database Administrator Activities 28](#_Toc52287945)

[4.4.6 Data Governance 28](#_Toc52287946)

[4.4.7 Data Management 28](#_Toc52287947)

[4.4.8 Data Architecture 28](#_Toc52287948)

[4.4.9 Production Database Change Requests 29](#_Toc52287949)

[4.4.10 Configuration Releases (Patching) 29](#_Toc52287950)

[5. SECTION 508 – ACCESSIBILITY OF INFORMATION AND COMMUNICATIONS TECHNOLOGY 30](#_Toc52287951)

[5.1 Section 508 Accessibility Standards 31](#_Toc52287952)

[5.1.1 Software Development, Software Applications and Operating Systems 32](#_Toc52287953)

[5.1.2 Web-based Applications 32](#_Toc52287954)

[5.1.3 Telecommunication Products and Services 32](#_Toc52287955)

[5.1.4 Video and Multimedia Applications 33](#_Toc52287956)

[5.1.5 Self-Contained and Closed Products 33](#_Toc52287957)

[5.1.6 Desktop and Portable Computers 33](#_Toc52287958)

[5.1.7 Help Desk and Other Support Services 33](#_Toc52287959)

[5.1.8 WCAG 2.0 Compliance 34](#_Toc52287960)

[5.1.9 Non-Compliance 35](#_Toc52287961)

[5.2 ICT Accessibility Requirements Statement per the Revised Section 508 of the Rehabilitation Act 35](#_Toc52287962)

[6. INTELLECTUAL PROPERTY AND KNOWLEDGE TRANSFER 36](#_Toc52287963)

[6.1 Knowledge Transfer 36](#_Toc52287964)

[6.2 Recording and Disclosure of Contract Intellectual Property 36](#_Toc52287965)

[6.3 Cooperation with other Service Providers 36](#_Toc52287966)

[6.4 Email 36](#_Toc52287967)

[7. APPLICABLE DIRECTIVES 37](#_Toc52287968)

[7.1 Industry Standards 37](#_Toc52287969)

[7.2 Other Federal Government and USDA Requirements 37](#_Toc52287970)

[7.3 Compliance with Internet Protocol Version 6 (IPv6) 38](#_Toc52287971)

[8. PERIOD OF PERFORMANCE 38](#_Toc52287972)

[9. KEY PERSONNEL REQUIREMENTS 39](#_Toc52287973)

[9.1 Senior Project Manager 40](#_Toc52287974)

[9.2 Senior System Architect/Technical Lead 40](#_Toc52287975)

[9.3 Senior Database Administrator 40](#_Toc52287976)

[9.4 Senior Production Support Lead/Data Analyst 41](#_Toc52287977)

[9.5 Senior Developer 41](#_Toc52287978)

[9.6 Senior Business Analyst 41](#_Toc52287979)

[9.7 Senior Software Developer 42](#_Toc52287980)

[9.8 Database Administrator 42](#_Toc52287981)

[9.9 Database Architect 42](#_Toc52287982)

[10. DELIVERABLES 43](#_Toc52287983)

[10.1 Documentation Submitted with the Proposal 43](#_Toc52287984)

[10.2 Progress Reports, Program Reviews and Status Reports 44](#_Toc52287985)

[10.2.1 Progress Reports 44](#_Toc52287986)

[10.2.2 Program Review 44](#_Toc52287987)

[10.2.3 Weekly Status Reports 44](#_Toc52287988)

[10.3 Fully Commented Source Code Delivery 44](#_Toc52287989)

[10.4 Programmatic Deliverables 45](#_Toc52287990)

[10.5 Continual Maintenance Deliverables 47](#_Toc52287991)

[11. CONSTRAINTS 48](#_Toc52287992)

[12. BILLING 49](#_Toc52287993)

[12.1 Submission of Invoices 49](#_Toc52287994)

[13. PLACE OF PERFORMANCE 50](#_Toc52287995)

[14. PERFORMANCE METRICS 50](#_Toc52287996)

[APPENDICES 55](#_Toc52287997)

**List of Tables**

[Table 1 – OIT Organization Information 16](#_Toc52287998)

[Table 2 - Requirement Types 18](#_Toc52287999)

[Table 3 - Vulnerability Response Time 25](#_Toc52288000)

[Table 4 – Telephone Line and Voice Response Times 28](#_Toc52288001)

[Table 5 – Email Response Times 28](#_Toc52288002)

[Table 6 - Programmatic Deliverables 47](#_Toc52288003)

[Table 7 - Continual Maintenance Deliverables 48](#_Toc52288004)

[Table 8 - Performance Metrics 54](#_Toc52288005)

[Table 9 – Appendices 55](#_Toc52288006)

**ACRONYM LIST**

*List the acronym reference and definition or description for each acronym contained in this document.*

| **REFERENCE** | **DEFINITION** |
| --- | --- |
| A&A | Assessment and Authorization |
| ACR | Accessibility Conformance Report |
| AQL | Acceptable Quality Level |
| ATO | Authority to Operate |
| BOD | Binding Operational Directive |
| BPA | Blanket Purchase Agreement |
| CCB | Change Control Board |
| CCR | Centralized Code Repository |
| CDM | Continuous Diagnostics and Mitigation |
| CDMP | Certified Data Management Profession |
| CEC | Client Experience Center (CEC) |
| CER | Change Enhancement Request |
| CFR | Code of Federal Regulations |
| CISSP | Certified Information Systems Security Professional |
| CM | Configuration Management |
| CMD | Contracts Management Division |
| CMMI | Capability Maturity Model Integration |
| CO | Contracting Officer |
| COBIT | Control Objectives for Information and Related Technology |
| COOP | Continuity of Operations Plan |
| COR | Contracting Officer’s Representative |
| COTS | Commercial off-the-shelf |
| CPIC | Capital Planning and Investment Control |
| CSP | Certified Scrum Practitioner |
| CUI | Controlled but Unclassified |
| DBA | Database Administrator |
| Dev | Development |
| DHS | Department of Homeland Security |
| DISC | Digital Infrastructure Services Center (DISC) |
| DUNS | Data Universal Numbering System |
| EIT | Electronic and Information Technology |
| FAR | Federal Acquisition Regulation |
| FIPS | Federal Information Processing Standards |
| FISMA | Federal Information Security Modernization Act |
| FMS | Financial Management Service |
| FNS | Food and Nutrition Service |
| GFE | Government Furnished Equipment |
| HRBAC | Hybrid Role Based Access Controls |
| HSTS | Hypertext Transfer Protocol (HTTP) Strict Transport Security |
| HTTP | Hypertext Transfer Protocol |
| HTTPS | Hypertext Transfer Protocol Secure |
| ICCP | Institute for Certification of Computing Professionals |
| ICT | Information and Communications Technology |
| IEEE | Institute of Electrical and Electronics Engineers |
| IMS | Integrated Master Schedule |
| INTEG | Integration |
| IP | Intellectual Property |
| IPP | Invoice Processing Platform |
| IPT | Integrated Project Team |
| IRP | Incident Response Plan |
| IRR | Integration Readiness Review |
| ISO | International Organization for Standardization |
| ISO | Information Security Office |
| IT | Information Technology |
| ITI | Information Technology Industry |
| ITIL | Information Technology Infrastructure Library |
| IV&V | Independent Verification and Validation |
| Jira | Jira is a proprietary issue-tracking and project management tool, developed by Atlassian. |
| LOE | Level of Effort |
| MBI | Moderate Risk Background Investigation |
| MS | Microsoft |
| NIST | National Institute of Standards and Technology |
| NLT | No Later Than |
| ODC | Other Direct Cost |
| OIT | Office of Information Technology |
| OMB | Office of Management and Budget |
| OS | Operating system |
| PII | Personally Identifiable Information |
| PL | Public Law |
| PM | Project Manager |
| PMD | Portfolio Management Division |
| PMI-ACP | Project Management Institute’s Agile Certified Practitioner |
| PMP | Project Management Plan |
| POA&M | Plan of Action and Milestones |
| PPA | Project Process Agreement |
| PWS | Performance Work Statement |
| QA | Quality Assurance |
| SAR | Supplemental Accessibility Conformance Report |
| SDD | System Design Document |
| SDLC | Systems Development Lifecycle |
| SEI | Software Engineering Institute |
| SIEM | Security Information and Event Management |
| SLA | Service Level Agreement |
| SME | Subject matter expert |
| SNAP | Supplemental Nutrition Assistance Program |
| SORN | System of Record Notice |
| SQL | Structured Query Language |
| SRS | System Requirements Specification |
| STIG | Security technical implementation guide |
| TBD | to be determined |
| TFS | Team Foundation Server |
| U.S.C. | United Stated Code |
| UAT | User Acceptance Test(ing) |
| USDA | United States Department of Agriculture |
| VDD | Version Description Document |
| VPAT | Voluntary Product Accessibility Template |

# PURPOSE

*Insert a brief introduction here. Update with general, high-level introduction describing the purpose/intent for this project and how it supports the organization’s mission and strategic goals. See below for example.*

The United States Department of Agriculture (USDA), Food and Nutrition Service (FNS), Supplemental Nutrition Assistance Program (SNAP) has expanded the use of data analytics and business process reengineering in the area of program integrity over the last few years. The insights and lessons gleaned from the prior work are driving a desire to expand the use of these and other similar analytical processes out to other areas of the program. Doing so enhances the government’s ability to make data-driven decisions in the program analysis and administration of SNAP. To that end, FNS requires a platform to house, and consolidate and analyze internal and external data.

# BACKGROUND

*Insert background information according to project needs, starting with the Department/Agency and drilling down into the Program/Division. Insert organization charts, tables, and diagrams, if possible. Add as many subsections as necessary to provide background information.*

# SCOPE

*The following subsections were embedded in prior PWS language/tasks. Agile Development Methodology is outlined in detailed in this section and referred to in development activities. You may keep these subsections under scope or move to other sections within your PWS document for clarity or flow purposes.*

This PWS describes in detail the contractor support and services required for <Application/System Name>, including project management; communications and stakeholder engagement; requirements/user story management; system design, system and reports development, testing, security, and implementation; continuous system monitoring; and user support.

The contractor shall follow the Agile Development Methodology and other requirements and guidance below. Specifically, the following subsections provide information for Agile Development Methodology, Security, Quality Assurance and Configuration Management, SDLC Oversight, IT Policies and Procedures Support; Compliance with Applicable Laws, Regulations and Standards; General IT Security and Privacy Requirements and Data Rights.

## Agile Development Methodology

*Keep this subsection for projects containing agile development activities, whether new development or sustainment activities.*

The contractor shall utilize an Agile Software Development methodology, Scrum preferred, and the associated industry leading practices and automated tools to keep historic records of all Sprint-related activities. The contractor shall develop and propose a Product Roadmap for this development project in which Sprints do not exceed 4-weeks in duration, provides for quarterly software releases, and utilizes automated tools that maintain, generate, and track the Product Backlog, Sprint Backlog, Velocity Charts, Burndown Charts, Bugs/Issues, and Risks for the life of the project.

### Backlog Management and Estimation

The contractor shall provide story point / level of effort estimations in the product backlog on an ongoing basis to ensure a minimum of 1.5 to 2 sprints worth of change requests/users stories have been estimated at any given time based on Product/Business Owner prioritization. Requirements/user stories may be refined adaptively over the course of the effort to continuously meet specified user needs. User needs will be prioritized based on business value and technical dependencies and maintained in the <Application/System Name> FNS Jira project.

For the benefit of both FNS and the contractor all requirements shall be groomed as user stories and put into the backlog. The living backlog represents all requirements past, present, and future of <Application/System Name>. The contractor shall work with the FNS Project team to develop, enhance, and manage user stories based on the backlog. Decisions to add, delete, or modify user stories shall involve the integrated project team; however, all decisions will be approved by the COR.

Requirements shall be identified, agreed to between the COR and the contractor, and approved for a release in a planning meeting prior to the production deployment of the previous release.

### Sprint

The contractor shall deliver the software design, development, and testing in 2-4 week sprints that produce discernible, incremental progress deliveries and COR-approved production ready software. COR/Business Owner expect these deliveries of capabilities shall be implemented in the production environment. The overall time required to deliver production ready software is dependent on release planning, complexity of features, themes and epics, based on a fixed time cycle, with variances in the amount of features developed. The contractor shall use continuous integration best practice techniques in developing software solutions. The contractor shall ensure adequate delivery in both cases. All deliveries shall adhere to FNS Office of Information Technology (OIT) SDLC guidelines.

The overall time required to deliver production-ready deliverables is dependent on the release planning, complexity of features, themes and epics, based on a fixed time cycle, with variances in the amount of features developed.

The contractor shall follow the FNS Systems Development Lifecycle (SDLC) and shall follow all FNS procedures for moving the system into the UAT and production environments. The contractor shall also be responsible for implementing the final code into the backup environment.

### Sprint Review/Demonstrations

The contractor shall conduct a Sprint Review for all items that have been completed (developed and tested) at the end of each Sprint and discuss user stories that were identified for the Sprint and not completed. Each completed user story is presented to the Product Owner (PO), and the PO either accepts or rejects the changes. User stories that are accepted by the PO are staged for release. Any items that are rejected by the PO or not completed are placed back into the Product Backlog for future analysis and prioritization.

The contractor shall provide a demonstration for all user stories in a given release prior to the beginning of User Acceptance Testing (UAT).

*You may want to include the below paragraph if this PWS is for a New Agile project to allow sufficient response time for potential changes prior to the initial release, especially if the project is of large-scale.*

The contractor shall provide an in-depth walk through of the functions when roughly three-fourths of the way through the Theme or Epic level changes for the release. This is intended to provide the Government an opportunity to ensure such a sweeping change is going in the correct direction, while at the same time allowing the contractor sufficient development to be able to present meaningful content. An interactive meeting showing design, and progress towards goals is required. This meeting shall be a part of the applicable Release Schedule, outside of normal weekly meetings, and can be scheduled by the contractor from the point of the scheduling purposes. The meeting shall be long enough to cover the materials and allow for in-depth questions or demos. This is a pre-UAT for the release, as such, the COR will be returning feedback to the contractor. Adjustments based upon this feedback will be inserted at points negotiated in the meeting, or in a future Sprint per the standard change methods.

### Metrics and Reporting

The contractor shall maintain status and traceability metadata information for each system / application change in the <Application/System Name> FNS Jira project to include the following at a minimum:

* Status
* Sprint
* Release
* Test Case(s)
* Epics/Themes
* Design artifacts (if applicable)
* Story Point / LOE estimation
* Acceptance Criteria

The contractor shall configure the FNS <Application/System Name> FNS Jira project to provide agile metrics that focus on the delivery of software to include the following at a minimum:

* Sprint Burndown
* Release Burndown
* Velocity
* Control Chart
* Sprint Report
* Cumulative Flow Diagram

Contractor shall provide the COR an end-of-Sprint report at the end of each Sprint detailing the user stories that were addressed in a format approved by the COR.

## Security

*This section is required for all PWSs that have System Development or Sustainment activities. Tailor last paragraph to fit your contract specific needs and description.*

The scope of this contract includes any activities necessary to actively monitor system security, prevent security incidents, respond to security incidents, or to remediate security vulnerabilities within the platform. Security includes responsibility for safeguarding data transferred to and from the platform and shall adhere to NIST SP 800-171 Protecting Controlled Unclassified Information in Nonfederal Systems and Organization (see Appendix E), as well as physical security and access controls to the platform. All traffic will use secure transfer protocol and encryption (e.g. HTTPS, with HSTS) and comply with the latest directive where applicable. (E.g. Binding Operational Directive 18-01 (BOD 18-01) (see Appendix F) and Office of Management and Budget Memorandum-15-13 (OMB M-15-13) (see Appendix G).

Furthermore, FNS internal systems include personal identifying information (PII) about SNAP program recipients and retailers participating in the program. FNS intends to bring in additional external data sets, which also contain PII data on SNAP recipients. As a result, the ability to mask and scramble PII data on all environments (e.g. Development, Pre-Production, Production, etc.) and create new unique identifiers in lieu of PII data to support business needs (ex., replacing SSN with a new unique identifier where applicable) are considered within the scope of security for this contract.

## Compliance with Applicable Laws, Regulations, and Standards

*This section is required for all PWSs.*

* **Federal Laws**. The contractor and all of its respective subcontractors shall follow and remain compliant at all times with the Federal Acquisition Regulation (FAR), Privacy Act of 1974 (5 U.S.C. 552a - the Act), Federal Information Security Modernization Act of 2014 (Public Law 107-347) (FISMA) as applicable.
* **FIPS and NIST Special Publications**. The contractor and all of its respective subcontractors shall follow Federal Information Processing Standards (FIPS), National Institute of Standards and Technology (NIST) standards and guidelines, and other laws, mandates, or executive orders pertaining to the development, operations, and protection of information systems and sensitive information and data.
* **USDA and FNS Policies and Procedures**. The contractor and all of its respective subcontractors shall comply with all USDA and FNS security and privacy policies and standards in effect at the time of the award of the contract, as well any requirements added during the contract.
* **Privacy Act**. As prescribed in the FAR 24.104, as the contract involves the design, development, and/or operation of a system of records on individuals, the contractor must implement requirements in FAR clause 52.224-1, “Privacy Act Notification” and FAR clause 52.224-2, “Privacy Act” in coordination with FNS. In addition, the contractor is responsible for training of individuals supporting FNS in accordance with FAR clause 24.301, “Privacy Training.”
* **Telecommunications and Video Surveillance Services or Equipment.** The contractor and all of its respective subcontractors shall follow and remain compliant at all times with the FAR clause 52.204.24 Representation Regarding Certain Telecommunications and Video Surveillance Services or Equipment and FAR clause 52.204-25 - Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment.

## General IT Security and Privacy Requirements

*This section is required for all PWSs.*

* **Authorization to Use, Store, or Share Sensitive Information**. The contractor shall be responsible for properly protecting all information used, gathered, or developed as a result of work under this contract. The contractor shall also protect all government data, equipment, etc. by treating the information as sensitive. The contractor shall consider all information about the system, gathered or created under this contract as Controlled but Unclassified (CUI) information. This information will be gathered, created, and stored only on the FNS network using FNS Government Furnished Equipment (GFE). The contractor shall use of any information that is subject to the Privacy Act in full accordance with all rules of conduct as applicable to Privacy Act Information.
* **Deliverables**. The deliverables in this contract are sensitive and are not shareable with any other organization without prior approval from the FNS CO.
* **Confidentiality**. The contractor agrees to assume responsibility for protecting the confidentiality of government records and data associated with this contract, which are not public information. Each contractor or employee of the contractor to whom information may be made available or disclosed shall be notified in writing by the contractor that such information may be disclosed only for a purpose and to the extent authorized herein.
* **Non-Disclosure Agreement**. Each individual who has access to FNS or USDA facilities under this contract shall execute a Non-Disclosure Agreement before accessing FNS or USDA facilities under this contract.
* **Need to Know**. Sensitive information, data, and/or equipment will only be disclosed to authorized personnel on a Need-To-Know basis. The contractor shall establish appropriate administrative, technical, and physical safeguards to properly protect the security and confidentiality of this information, data, and/or equipment.
* **Use of PII**. The contractor shall not use any Personally Identifiable Information (PII), E-mail Groups, Lists, or contract information for any purpose other than those activities necessary to the performance of this contract.

## Required Development Practices

*This section is mandatory for development/Sustainment tasks.*

In addition to the Agile Development Methodology noted above, the contractor shall adhere to the practices outlined in the below subsections when developing capabilities to be assessed through independent scanning and testing of implemented security controls.

### Standards

The contractor shall ensure compliance with the applicable NIST 800-53 controls, and USDA policies for Safeguarding Sensitive but Unclassified Information (NIST SP 800-171, also referred to as CUI). The contractor shall provide IT security support for configuration management, change request process, and the evaluation of technical designs during the engineering process.

### Development Practices

1. If the contractor must perform changes to code, they must develop and deliver the software components and documentation to address functional and system requirement changes, ensure approval of the technical design, and meet end-to-end performance requirements. The contractor shall conduct unit testing prior to delivery to any UAT environment.
2. Code Review/Testing: The contractor shall perform code review to discover and resolve defects before it is tested. The contractor shall utilize automated secure code test/analysis tools (as provided by the government) and make the results of such testing available for review and approval by the government with delivery of each release.
3. Minimize Attack Surface Area: The contractor shall document new features, new code, and all configuration changes; assess and clearly document the impact on current level of risks i.e. whether the new features increase or decrease the risk.
4. Source Code: The contractor shall digitally sign all applicable source code; ensure digitally signed source code by the designated development authority; and allow only signed code to execute on FNS or designated hosting facility. Further, all source code delivered must be placed into the FNS Enterprise Team Foundation Server (TFS) Centralized Code Repository (CCR).
5. Mobile Code: The contractor shall digitally sign all mobile code; ensure digitally signed mobile code by the designated USDA FNS authority; and allow only signed code to execute on <Application/System Name>.
6. Personal Identifying Information: <Application/System Name> may provide access to data that may contain Personal Identifying Information (PII) data on SNAP recipients. As a result, the ability to mask and scramble PII data on all environments (e.g. Development, Pre-Production, Production, etc.) and use new unique identifiers in lieu of PII data to support business needs (e.g., replacing Household and Card Numbers with a new unique identifier where applicable) are considered within the scope of security for this contract.
7. The contractor shall deliver the software code to include executables, scripts, source code, configuration files, test scripts, and any commercial off-the-shelf (COTS) products with associated license keys and documentation to the FNS Enterprise TFS CCR at every <identify frequency – every release or every major> release.
8. The contractor shall utilize the designated FNS-provided repository to preserve the code base and conduct a walkthrough with the government prior to delivery of the release code baseline. The contractor shall be responsible for maintaining (hardware, software, and associated documentation) and utilizing the FNS provided development environment consistent with the FNS architecture framework.
9. The contractor shall ensure that the software development efforts (up to code freeze to support software delivery) are void of any deficiencies associated with performance/integration, don’t break non-related functionality, and addresses applicable security vulnerabilities.
10. The contractor shall utilize FNS approved software to evaluate the quality of the code delivered during the integration process. Code must undergo quality review prior to being introduced into <Application/System Name> codebases. This quality review must include static code analysis and automated unit testing. Code shall be analyzed to 1) identify and track quality issues; 2) provide the data to monitor development performance; 3) measure quality and adherence to architectural and coding standards; 4) provide metrics for development strategy; 5) scanning for vulnerabilities; 6) ensuring Section 508 compliance; 7) measuring cyclomatic complexity (with target </=10); and 8) compatibility with FNS standard operating system (OS) and browser configurations. During development, the contractor shall incorporate the use of a tool(s) into their internal development processes to include but not limited to; 1) developer feedback; 2) peer reviews; and 3) internal milestone reviews. If code does not comply, it is unacceptable for delivery.

### Security Practices

1. Separation of Duties: The contractor shall design, build, and maintain segregation of duties into their roles, environments, and applications. The contractor shall design applications to recognize conflicts between individual duties. Privileged account holders must act in accordance with FNS Rules of Behavior outlined in the FNS-702 Handbook.
2. Identification/Authentication/Authorization/Accountability: The contractor shall design and develop procedures for Identity Management utilizing USDA standard Identification and Authentication infrastructure, processes and policies. The contractor shall also implement Hybrid Role Based Access Controls (HRBAC) and segregation of duties via these procedures.
3. Secure Coding Standards: The contractor shall follow USDA Secure Coding Standards in development of any code.
4. Data Encryption. Data Encryption: The contractor shall implement security mechanisms that are FIPS 140- 2 compliant to support Preservation of Information and System Confidentiality, Integrity, and Non-Repudiation. Where encryption is required, as specified by FNS, the contractor shall ensure that encryption is established and maintained for data at rest and in transit for the duration of the contract. The encryption employed shall be equivalent to those approved in Federal Information Processing Standards (FIPS) Publication 140.
5. Secure Configurations: The contractor shall not deploy applications with default (i.e. "out of the box") security configurations. The contractor shall secure the application configuration and change all default passwords and all default settings. The contractor shall apply FNS-approved secure baseline configurations to all IT components of the system. Secure configuration settings must be define, implemented, and maintained in accordance with NIST, USDA, and FNS requirements, to include NIST Special Publications 800-70 and 800-53 (current Revisions).
6. Principle of Least Privilege: The contractor shall apply the principle of least privilege in performing their processes. The contractor shall develop applications consistent with this principle and allow for fine-grained access privileges.
7. Fail Securely: The contractor shall design and develop applications to fail securely. Applications shall not be exploitable in failure conditions.
8. Security Issues Mitigation: The contractor shall remediate all security issues identified during the certification, authorization, or other risk assessment processes within a mutually agreed upon timeframe.

The contractor shall also, as part of solution development and updates:

1. Provide a description of the functional properties of the security and privacy controls employed by the system, for inclusion in the associated Authorization Package documentation. Per Office of Management and Budget (OMB) Circular A-130, the Authorization Package includes the information system security plan, privacy plan, security and privacy control assessment, and any associated plans of action and milestones (POA&M).
2. Provide design and implementation information for the security controls to be employed that includes: all external system interfaces, high- and low-level design, source code and hardware schematics, and design and implementation information at a level commensurate with that specified in the FNS SDLC and consistent with all NIST controls applicable to the FNS information resources displayed, processed, stored or transmitted.
3. Identify early in the system development life cycle the functions, ports, protocols, and services intended for FNS use.
4. Provide administrator documentation for the information system that describes: (1) secure configuration, installation, and operation of the system, component or service; (2) effective use and maintenance of security functions/mechanisms; and (3) known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions.
5. Provide user documentation for the information system that describes: (1) user-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms; (2) methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner; and (3) user responsibilities in maintaining the security of the system, component, or service.

### Performance and Monitoring Practices

1. Logging/Monitoring: The contractor shall implement functionality in the applications that sends security-related and other relevant alerts to the FNS logging/monitoring infrastructure in accordance with USDA Cybersecurity policy.
2. Performance Monitoring: The contractor shall enable applications and application infrastructure to generate events and alerts as specified by the FNS; shall support the capture and analysis of the application alerts and events; and shall support the integration of these alerts and events with the FNS-provided mechanisms. FNS utilizes Splunk for managing monitoring logs.
3. The contractor shall configure the application and supporting IT components per FNS direction, to forward designated audit logs to the FNS Security Information and Event Management (SIEM) tools for monitoring operational activities.

### Cloud Practices

Using Cloud Services: Should the selected solution employ the use of a Cloud, the contractor shall provide a solution that meets all FedRAMP (Appendix C), USDA, and FNS security requirements. FNS OIT will determine the appropriate hosting environment based upon the requirements, the security rating and proposed design.

## Quality Assurance and Configuration Management

*In addition to the example below, it is recommended to include language that specifies all documents should be of professional business-quality and peer-reviewed prior to submission.*

Hardware or software configuration changes shall be in accordance with the FNS standards and the FNS Continuous Diagnostics and Mitigation (CDM) Program. The FNS Change Control Board (CCB) shall approve any request for change prior to any development activity occurring for that change and shall define the security and functional requirements for the requested change.

The contractor shall fully document all development and changes to the production system as outlined in Appendix A, FNS Agile Systems Development Lifecycle Guide. The contractor shall ensure that all code is version controlled and has successfully passed an independent code review prior to any production release. The contractor shall make available documented evidence of independent code reviews to the government upon request. Coding support shall include ensuring that configuration management (CM) processes and procedures are adhered to and in place for the continued development of the system. CM shall include code control in all the system environments, which may include the development (Dev), QA, pre-production/integration (INTEG)/user acceptance testing (UAT), production, and disaster recovery environments. Any changes to CM practices must first receive written approval from the COR. The COR will then seek consultation with the appropriate USDA entity (i.e., Information Security Office (ISO), FNS OIT, etc.).

QA tasks also include testing the application, finding and reporting bugs in the code, preparation of test cases, and preparation of test plans. The vendor must select, as part of their proposal process, automated testing tools that they will utilize with a preference towards tools specified in the FNS Approved Software List (Appendix I). For non-open source software, provide licensing charges as an Other Direct Cost (ODC) in the proposal. Where applicable, the contractor shall ensure the successful transfer of data/information from the source destination to its final resting place. The contractor shall also be responsible for all data validation and any required data cleansing resulting from user activities such as import/export, data conversion, data migration, manual data entry, etc. that corrupted the system. QA tasks also include coordination of various levels of testing (such as application testing, functionality verification, load testing, independent QA testing, and thorough regression testing) during releases and patch or other server upgrades. It shall also include the creation of bi-directional traceability between new requirements/user stories and test cases. CM tasks include plan development and updates, configuration identification, configuration change control, and baseline management.

When applicable, the contractor shall also be responsible for providing the code for implementation in the User Acceptance Test (UAT) environment and providing support to FNS and the hosting site for integration and implementation into the production environment. FNS may provide a production mirror site for contractor-led testing prior to production release, if necessary.

## Data Rights

*This section is required for all PWSs.*

The Government has unlimited rights to all documents/material produced under this contract. All documents and materials, to include the source codes of any software, user stories, UAT, documentation, etc. produced under this contract shall be Government owned and are the property of the Government with all rights and privileges of ownership/copyright belonging exclusively to the Government. These documents and materials may not be used or sold by the contractor without written permission from the Contracting Officer. All materials supplied to the Government shall be the sole property of the Government and may not be used for any other purpose. This right does not abrogate any other Government rights.

# PERFORMANCE AND TASKS

*Insert description of required Performance and Tasks according to project needs (By Tasks, By Phase, New Agile project or an existing Agile project, etc.). Describe each Task or Phase in detail. There are multiple sections below for your use in developing the PWS.*

*If project is for Development or Enhancement, the description should specify overall goal that Product/Business Owner hopes to achieve from this project. This is high-level, provided by the Product/Business Owner, and reviewed by PMD or appropriate Branch.*

***New Agile Projects***

The contractor shall work directly with FNS’s Office of Information Technology (OIT) and various programs who partner with OIT for project management support to identify requirements, and design and build robust applications that supports the agency’s business processes and activities. The work included in this Task Order will focus primarily on identifying and documenting the requirements necessary for configuring the platform/environment and designing and developing the initial application.

FNS sees the project as taking place over three phases. The first two phases, included within this Task Order, includes Phase 1 which encompasses Requirements Definition and Design and Phase 2 which includes platform configuration and application development using an Agile Development Methodology noted above. Phase 3, which is out of scope for this Task Order, will include task orders for O&M and enhancements.

***Existing Agile Projects***

The contractor shall work directly with FNS’ Office of Information Technology (OIT) and <Program/Business Office information> to accomplish the tasks within the Performance Work Statement (PWS). The following detailed tasks together constitute this PWS:

* Task A - Program Management Support
* Task B - System Development
* Task <X – Sustainment>
* Task <X - Help Desk Support>
* Task <X - Transition Support>

## Project Management Support

*This section is a requirement for all PWSs. Describe details of project management support needed for both Development and Sustainment needs as necessary. See below for example. Include all subsections below to some extent.*

The Government seeks a subject matter expert with Program Management capability that establishes and maintains program management practices throughout the period of performance. Program Management practices shall provide visibility into the contractors’ organization and techniques used in managing the Program, specifically subcontractor and data management. Documentation shall be readily available to Government representative(s) upon request.

The contractor shall provide the planning, direction, coordination, and control necessary to effectively and efficiently accomplish all design, development, implementation, operations, and reporting activities in accordance with the contract, and in alignment with USDA FNS SDLC processes and procedures. Project Management Support involves oversight tasks performed by the project manager to ensure the design, development, testing and deployment tasks are executed successfully and with quality, using the Capability Maturity Model Integration (CMMI), International Organization for Standardization (ISO), or other Industry Standard Quality Assurance practices by the team on a consistent basis. Key components of this task include ensuring appropriate communication channels are established and maintained with the FNS OIT, the COR, Business Owners, other members of the integrated project team and stakeholders through the use of routine status reports, real-time updates and virtual/physical ad hoc and regularly scheduled meetings.

The contractor shall maintain a Project schedule that shall include all significant events, and a Project Planning Milestone Chart that depicts major tasks and events from start to completion of the contract. The contractor shall notify the Government in writing within one (1) business day of any anticipated or projected work stoppages or delays that will impact schedules. The contractor shall not implement any decisions that will affect work or schedules without the consent of the COR. When the FNS National Office closes due to inclement weather, FNS expects that the contractor shall carry out normal development, O&M, and user support tasks. Notification of these stoppages can occur through documented weekly reports.

### Project Manager Support

The contractor Project Manager (PM) shall ensure the timely accomplishment and quality completion of all related project tasks and delivery of all contract deliverables, At a minimum, the contractor PM shall provide both weekly and monthly status reports which shall describe the status/progress of Tasks <X> through <X> including project schedule, problems encountered and known risks, along with proposed solutions and impacts.

The contractor PM shall provide oversight for the <Application/System Name>, Project Management Support, and Information Technology (IT) System Development best practices, methods, and tools in compliance with USDA/FNS OIT policies and protocols, including the FNS Agile Systems Development Lifecycle Guide (SDLC) (Appendix A).

The contractor PM shall:

* Provide daily project leadership and guidance to the contractor team.
* Participate in all Integrated Project Team (IPT) meetings; including additional scheduled FNS stakeholder meetings with the contractor team.
* Develop and maintain a detailed project management plan (PMP), which includes the risk management plan.
* Accountable for the entire project lifecycle, including roadmap planning and release planning/management.
* Develop and maintain a detailed project schedule.
* Develop and maintain weekly progress reporting.
* Develop and maintain monthly progress reporting.
* Host weekly and monthly status meetings with the integrated project team, inclusive of additional FNS stakeholders and the contractor team.
* Coordinate and/or attend technical interchange meetings.
* Establish appropriate communication channels between the various project stakeholders, provides routine status reports (weekly and monthly), and conducts meetings with FNS and Product/Business Owners to keep them updated on all project activities and any risks/issues.
* Capture and release to the IPT meeting minutes and action items (i.e. during formal interactions with the Project Area, Product/Business Owners, Information Security Office (ISO), OIT, internal/external agencies, etc.), and tracking action items to completion.
* Resolve cross-functional issues at the project-level.
* Anticipate stakeholder needs and works with Product/Business Owners to successfully manage changes in project scope, schedule, budget, and personnel;
* Manage project scope and reporting issues; escalating matters to the COR when necessary.
* Ensure successful execution of tasks and with quality (using CMMI level II, SDLC, and other quality assurance (QA) best practices) by the team on a consistent basis.
* Create and manage the Project Risk and Issue Registers.
* Provide documentation of the detailed project plan and technical documentation, in accordance with FNS OIT SDLC, instructions, policies, and protocols.
* Manage project deliverables according to the project plan and roadmap milestones.
* Capture, monitor, and review team productivity to drive continuous improvements and high quality performance.
* Work closely with FNS OIT and other identified stakeholders to ensure the project milestones and deliverables meets business, functional and non-functional requirements expressed as user stories, as well as user expectations.
* Provide updates to the Continuity of Operations Plan (COOP), if required.
* Provide information needed for Assessment and Authorization (A&As) and information security solutions. This includes coordinating remediation of vulnerabilities, updating security documentation, and participating in continuity of operation exercises.

### Contractor Responsibility with Project Documentation

In order to effectively manage the project, the contractor shall work with various stakeholders, and identify, document, and lead recurring meetings. This includes coordinating and scheduling the various meetings, preparing and distributing one (1) full business day in advance read-ahead meeting agendas (for all regularly scheduled meetings), and providing detailed meeting minutes within two (2) business days following, which shall include, at a minimum:

* Meeting Title/Subject
* Scheduled Date and Duration (times)
* Facilitator and Scribe’s Name
* List of all Invitees, their specific role, and if attended (i.e., Yes or No)
* Executive Summary (with applicable background and purpose of the meeting)
* Agenda Topics
* Meeting Minutes (what was actually discussed and the decisions made)
* Action Items (with by-name assignment and due dates - tracked until completed)

The contractor shall capture meeting minutes and action items during formal interactions regardless of whom initiated the meeting (and regularly scheduled meeting) with the Program Areas, Product/Business Owners, ISO, OIT, COR, internal/external agencies, etc., and tracking action items until completed. The contractor shall track all action items on a consolidated Action Item Register for the project. Meeting minutes are due to the COR and <XXXXXX>, via email, within two (2) business days following the meeting.

The contractor staff shall also be responsible for the coordination among stakeholders in preparing, updating, tracking, and maintenance activities for all project-related documentations, and the Capital Planning and Investment Control (CPIC)/SDLC documentation located at Appendix B – <Application/System Name> Project Process Agreement (PPA).

The contractor staff shall support the completion of project-related security documentation such as Authority to Operate (ATO) and A&A documents.

Project documentation task objectives should include the following:

* Development, coordination, review, and delivery of project-related documentation and deliverables.
* Provide support and information to ISO for the completion of project-related security documentation.
* Create customer-facing documentation for technical enterprise software and developer tools.
* Document complicated procedures in simple and understandable manner and compose material according to set standards and templates.
* Coordinate, facilitate, write, edit, track progress, and package documentation for review and approval among the appropriate stakeholders.
* The contractor will place a copy of all project documentation in the FNS secure SharePoint portal.

### Decision Point Reviews

The contractor shall deliver Decision Point Review packages as laid out in the Agile Systems Development Lifecycle, Appendix A. Decision Point reviews are required for new development and quarterly releases, but not for emergency releases (bug fixes, patch releases, etc.).

* Build Decision Point - conducted after Sprint 0 to ensure that the project has successfully completed the all deliverables for this activity and there is a sufficient Product Backlog to begin the project. The <Application/System Name> Project Process Agreement (PPA) lists required documentation for Sprint 0. Refer to Appendix B – <Application/System Name> Project Process Agreement (PPA).
* Test Decision Point - occurs when all development and system testing has been completed and evaluates whether the project should proceed to the Test activity, specifically UAT and Independent Verification & Validation (IV&V) testing (if applicable). The <Application/System Name> Project Process Agreement (PPA) lists required documentation for Test. Refer to Appendix B – <Application/System Name> Project Process Agreement (PPA).
* Release Decision Point - occurs when all system testing has been completed, evaluated, and approved, including UAT and IV&V testing (if applicable), and the system is ready for a Go or No-Go. The <Application/System Name> Project Process Agreement (PPA) lists required documentation for Release. Refer to Appendix B – <Application/System Name> Project Process Agreement (PPA).

### Onboarding / Offboarding / Required Training

The contractor shall deliver Background Investigation (BI) forms for all personnel providing services to the Department. Forms shall be delivered to the CO or designee. Any personnel found to pose a risk or to be misleading in responses submitted in the BI documentation shall be removed at no cost or risk to the Department or the Agency. Decisions in this area are at the sole discretion of the CO and cannot be delegated. Additionally personnel found to be misusing government equipment shall similarly be removed from participation under this PWS at no cost to the Department or the Agency.

All personnel rolling off of the project or working on the project at completion shall complete and submit a Contractor Separation Form prior to the last billed day. All personnel participating under this PWS shall complete annual Information Security Awareness Training and all other training required for contractors providing technical services. Failure to fulfill this requirement may result in removal from participation under this PWS at no cost to the Department or the Agency.

### Escalation

It is in the government’s interest to be fair and equitable when dealing with the contractor. However in the unlikely event those differences cannot be overcome between the contractor and the CO, the contractor may choose to escalate an issue to the Chief of the Contract Management Branch. The Chief shall then manage the issue using Agency and Departmental policies and procedures.

## System Development

***New Agile***

***You can use the verbiage below for new agile projects. Tailor as necessary to include project specific information and requirements.*** *Ensure you add any project specific deliverables requested in the Deliverables section.*

The contractor shall use modular development, Scrum preferred, for this project in which tradeoffs (of user-stories) are not only allowed, but are expected. The contractor shall follow the FNS Agile Systems Development Lifecycle (SDLC) at the direction of the COR and shall follow all FNS procedures for moving the system into the UAT and production environments. The contractor shall also be responsible for implementing the final code into the backup environment.

The contractor shall:

1. Ensure the application operates in a secure manner reducing the risk exposure to the agency and the department and ensuring the confidentiality, availability and integrity of the data.
2. Complete security related training by specified deadline for all contract staff as needed.
3. Provide user stories, technical design, and architecture documentation for FNS review and approval if changes are required.
4. Use JIRA - an Agile Scrum automated issue tracking tool used at FNS that all Team members will have access to the tool.
5. Provide a release plan, outlining a Product Roadmap for future versions past the MVP (Minimum Viable Product).
6. Execute an implementation strategy that supports incremental business function and process migration with intermediate deliverables shipped on short timelines.
7. Cultivate a positive, trusting, and cooperative working relationship with the Government and other vendors that support FNS.
8. Ensure that FNS maintains ownership of and has ready access to all source code, databases, tests, documentation, deployment scripts, designs, user research documentation, and all other materials related to developing and deploying these capabilities. For Salesforce projects, databases must be distributed off of the platform and in government owned systems.
9. Leverage technology capabilities to meet customer needs with timely and seamless access to the cloud-based infrastructure, business applications, and data. This includes staying abreast of new feature offerings and new and innovative ways to provide technology value to agency customers, including, but not limited to, the Salesforce platform, open sourcing the applications, or the development of APIs.
10. Maintain a dialogue between the service provider and all project stakeholders, rather than trying to comprehensively specify requirements up-front. This focus will be assisted by working through short, tightly scoped product iterations in which working software is delivered to users regularly, and adjustments are made based on feedback gleaned from these iterations.
11. Lead and collaborate with the CORs, workgroups, and stakeholders in requirements sessions to develop recommendations and approaches, to be approved by the Government to satisfy the objectives and purposes of this contract. Results of these sessions will generate the Product Roadmap, Epics, Themes, and User Stories, business logic and rules, functionality, and system documentation.
12. Adhere to the Weekly Status Report documenting tasks & issues.

***Existing Agile***

*If this is an existing agile project, you may want to incorporate this language into this section in addition to the above language. Ensure you add any project specific deliverables requested in the Deliverables section.*

The contractor shall provide the development and support for improving and maintaining the capabilities of the system. The contractor shall incorporate the best practices of understandability, documentation, buildability, and interoperability into their development practice. The contractor shall produce quarterly releases (minimum of 4 per year), with the understanding smaller, emergency releases may be necessary. Each release will always have a Version Description Document (VDD), Release Notes, UAT Test Plan, and UAT sign-off. The contractor has the autonomy to determine their approach; however, following guidelines apply:

* Simplicity and unnecessary customization of codebases should be limited (understandability).
* Providing access to version control and commenting code in a way that it is understandable (documentation).
* Using tools for automated testing instead of relying on manual testing by the product owners (buildability).
* Utilizing open source libraries and frameworks without modifying too much of the functionality leading to simpler more interoperable code (interoperability).

### Requirements and Design

*The Requirements and Design section provides options to select from for requirements for your project.*

*New Agile Project – Phase 1 – Requirements and Design (and subsections) align with a phased approach for new development where requirements are gathered and developed to build a new application; while Existing Agile Project Requirements provide verbiage for development/enhancement within an existing system. Tailor language to fit your specific project needs, renumbering subsections as appropriate. For example, if choosing New Agile Project, this would become the Section 4.2.1 and subsections would be 4.2.1.1-4.2.1.5 respectively. If choosing Existing Agile Project Requirements, there would not be any subsections.*

#### New Agile Project - Phase 1 – Requirements and Design

*The following subsections can be used if this is a new Agile project, broken out by Phases or relevant. Adjust heading title and numbering as appropriate. Refer to Section 4.2.2 for information for Phase 2 – Development. Provide an explanatory paragraph for what the new application will provide to FNS. See example language below.*

The contractor shall create a high-level Requirements Document/Product Backlog, Future (To-Be) State Roadmap, and System Design Document that will be used to build and implement the <Application/System Name>.

The ability to access integrated, trusted data is integral to FNS achieving its mission. Many of the agency’s programs has data in disparate systems that, if combined, would enable analysis and insight that can better prepare staff to use data to better report, identify variances and trends, solve problems, and inform decisions.

*Example of explanatory paragraph.*

Implementing Salesforce across the agency provides a comprehensive set of tools and data for analysis in one place, allowing any authorized user to combine tools and data from multiple sources to answer questions that inform sound decision making. Leveraging Salesforce allows analysis to be performed without producing redundant activities. A “store once/use many” concept. A critical success factor is data governance to facilitate a planned, collaborative approach to making data management decisions that will account for both business and technical needs. In addition to the deliverables described in the subsequent sections, all deliverables identified in Appendix B, <Application/System Name> Project Process Agreement.

##### Requirements Document

*Describe what the requirements are for this project. For Sustainment, base requirements on maintenance of the project, whereas for new projects, base requirements on development of the system or application. Example below is for the development of a system or application.*

*Not all of the items below will be applicable to the project - add or delete additional requirement types as needed. Requirements document and Product Backlog are used interchangeably.*

The high-level Requirements Document/Product Backlog must bring together input from Chief Information Officer (CIO), three Portfolio Management Division branches and the Office of Policy Support described below, reflecting their collective input regarding the data and application requirements needed to fulfill area objectives.

##### OIT Organization Information

*Provide information for your project, if applicable. Change header title as needed. Below is an example.*

| **Area** | **Core Mission** |
| --- | --- |
| **Chief Information Officer** | Technology leaders delivering customer focused solutions. Enabling FNS programs to accomplish mission goals by:   * Committing to the excellence and success of its customers * Enacting proactive IT leadership with programs * Providing innovative and efficient solutions |
| **Portfolio Management** | Streamline IT business processes and optimize the FNS IT portfolio. Provide its customers both high-quality solutions and a standardized approach to obtain services. |
| **Program Management** | Provide Project Management, Customer Outreach, IT Contract Management and Program Management. |
| **Application Development** | Provide application consultation, custom application development, testing, and assurance along with maintenance support and enhancements services. |
| **Operations & Maintenance** | Oversees and conduct maintenance for all FNS applications and systems. Functions as liaisons to vendor for system  operations. |
| **Office of Policy Support** | Manage large portfolio of contracted research studies. |

Table 1 – OIT Organization Information

To ensure <Application/System Name> addresses and supports the collection of tools and data dependent tasks, duties and processes, Office of Information Technology (OIT) and the Office of Policy Support (OPS) should participate in defining the requirements. The vendor must produce a plan to collect input using interviews, workshops, surveys, etc. which can be decomposed and translated to requirements for use in user story creation, acceptance criteria definition and backlog management depending upon requirement type designation.

##### Requirements Types

*Use a Requirements Type table for both Development and Sustainment projects, with Sustainment maintaining the documentation required for this project. Tailor items within the table based on project needs since some of the items may not apply to your specific project, and add items as necessary.*

The below table identifies the requirement type and provides a description and example of the targeted requirement type for this project.

| **Requirement Type** | **Description**  ***Examples of Targeted Requirement Types*** |
| --- | --- |
| **Application/System** | Describes what the system must do in order to ensure that the solution operates correctly. These include regulatory/certification, business continuity and availability, service level objective, support, back-up and recovery, cyber-security, and system audit requirements.  *[Insert Example Here]* |
| **Reporting (general)** | Describes general reporting, analysis, and visualization of data requirements for the application/software/service.  *[Insert Example Here]* |
| **Metadata** | Describes metadata needed to support a successful implementation of the application/software/service. In some cases such as the look-up tables referenced in the requirements, the metadata is organized, managed, and available. In other cases, such as documenting the data schematics, the metadata will need to be captured or created. Document the level of sensitivity of the metadata (Controlled Unclassified Information, etc.)  *[Insert Example Here]* |
| **Temporal** | Describes needed currency of the data, the number of years of historical data to include, and the frequency of the data needed  *[Insert Example Here]* |
| **Data Quality** | Describes requirements for the quality of the data in the application/software/service, with emphasis on cited data concerns with the source systems.  *[Insert Example Here]* |
| **Enablement** | Describes user tools, training, and data understanding needed to get the most benefit from the application/software/service.  *[Insert Example Here]* |
| **Other Requirements** | Describes additional requirements necessary for effective implementation of application/software/service.  *[Insert Example Here]* |

Table 2 - Requirement Types

The high-level Requirements Document/Product Backlog serves as the foundation of the <Application/System Name> project, supporting and informing other project tasks including the assessment capstone - the Future (To-Be) State Roadmap for the <Application/System Name>.

##### Future (To-Be) State Roadmap

*Use this section for Development projects if you know the direction beyond the first Task Order. See example below.*

The Future (To-Be) State Roadmap describes recommendations (minimum 2 viable options) to achieve an end state that supports the requirements and is scalable to meet future Agency requirements. Furthering the goal of meeting future needs, the contractor shall design the <Application/System Name> so that it is capable of <insert description>. The following represents a sample list of sources to be considered in order to complete the Roadmap:

* Requirements Document/Product Backlog validated through workshops, interviews, surveys, etc.

And best practices in the areas of:

* Data Governance and data quality practices
* Data modelling practices
* Project Management Tools and Techniques
* Reporting practices
* Data integration practices
* Source System On-Boarding
* Hardware/Software Technologies
* Data security

The Future (To-Be) State Roadmap addresses the areas of:

* Reference Information Architecture Vision – Sources, acquisition, data integration, access, delivery, data lab, meta data, big data environment, audit controls.
* Information Architecture – conceptual, logical, semantic, physical data models, data modeling standards, temporal data, data security and privacy, master data management, data quality, subject areas.
* Application Architecture – Data integration, analytics, business objects migration, BI and data management software and services.
* Systems – Replication tools, data integration tools, analytics tools, system architecture diagram, enterprise data warehouse platform, big data environment and discovery platform, querying multiple repositories, data availability, development/test/disaster recovery environment, system performance capacity planning, workload management, job scheduling, security, systems management/monitoring.
* Enablement – Data governance, metadata management, user adoption, organizational support.
* Implementation process – requirements, solution architecture, data quality, logical, physical, access layer data modeling, data integration layer, analytic/BI solution, testing, and transition to production work streams.

The government will review the Future (To-Be) State Roadmap recommendations and the decisions made will inform the final System Design Document.

##### System Design Document

*For Development projects, see example below. For Sustainment projects, discuss as the maintenance of example below.*

The Future (To-Be) State Roadmap becomes the final System Design Document (SDD) after the government selects options made available and accepts subject matter expert (SME) recommendations.

#### Existing Agile Project Requirements and Design

*The following subsections can be used if this is an existing agile project that has new development or enhancements or the section is relevant. Adjust heading title and numbering as appropriate. See example language below.*

The contractor shall work with the Product/Business Owner, COR and stakeholders to elicit and document the requirements and design for <Application/System Name>. It is FNS’ desire that critical components, which are defined as “must haves” are included to the greatest extent possible in the minimum viable product (MVP). Inclusion of other major business components defined as “should haves” and “nice to haves,” will be prioritized accordingly. The contractor shall be responsible for documenting the requirements/user stories and business rules in Jira and providing screen mockups, recommendations, descriptions and business rules for the new / updated system functionality.

The contractor shall create/update the Product Backlog, Product Roadmap, and System Design Document for any major system enhancement as prioritized by the Product/Business Owner within the allocated sprint velocity. All requirement and design artifacts shall be presented to and approved by the Product/Business Owner before being added to a sprint for development / implementation.

### Development and Testing

*Rename this section based on type of project. For New Agile – Phased approach, name this Phase 2 – Development Support Services (or whatever is applicable). Tailor subsections to meet your project specific characteristics.*

The following subsections provide additional detail for development and testing activities to support the <Application/System Name> project.

#### Development

The contractor shall complete peer reviews while developing during each sprint. During the development process, the contractor shall ensure that the requirements/user stories and acceptance criteria are updated in JIRA in near-real time to reflect any changes and that the changes have been communicated and approved by the FNS Product Owner. The contractor shall adhere to USDA FNS SDLC processes and procedures, supporting Decision Point reviews as identified by the COR. The contractor shall ensure that JIRA status of each user story is updated within one (1) business day of any associated changes.

*Include this sentence if the project will not be using FNS’ e-Jira.* The contractor shall provide the Government with login credentials for five (5) end users to the contractor’s JIRA instance, allowing for review of all associated requirements/user stories in JIRA at any given time.

#### Testing

Testing in the agile development process requires frequent engagement with the customer and testers during design, system integration testing, and user acceptance testing. The contractor shall use the automated regression testing techniques and utilities as part of a continuous software integration process. Regression testing shall include testing to verify that new system updates do not introduce new bugs. The contractor shall ensure all products are thoroughly tested during each sprint prior to user acceptance testing and identify and correct product testing issues, especially during the critical period of integration testing for a releasable set of software features. Thorough, iterative testing includes unit, functional, system, interoperability, regression, security, and performance testing. The contractor shall provide testing and subsequent automated reports of browser compatibility and Section 508 compliance to ensure that all web pages and selected public-facing, print-ready reports or outputs are in compliance with Section 508 standards and best practices, as determined by FNS OIT.

For each sprint, the contractor shall create a test plan, inclusive of test scripts identifying Pass/Fail criteria. The contractor shall perform system integration testing (SIT) and manage the process of user acceptance testing (UAT), to include preparing for UAT with login accounts covering all user roles. The contractor shall schedule user acceptance kick-off meetings to provide an overview of the test scripts, demonstrate the requirements identified for user acceptance testing, and consolidate all test results via detailed session minutes. The contractor shall set up meetings to go over any system fails and what actions were taken to fix the issues.

Test scripts shall align with FNS OIT SDLC processes and procedures, and shall be developed before coding begins to support the test driven development. The contractor shall test the software throughout each sprint using industry best techniques, for both functional and non-functional requirements, including load, performance, and installation testing. The contractor shall correct and repair software defects throughout the agile software development process identified through all testing, including unit, functional, system, interoperability, regression, security, and performance, and conduct inspections and provide analysis of testing results as necessary to deliver production-ready code at the close of each sprint. Testing scripts, utilities, test execution, and testing results shall be historically maintained within JIRA and JIRA Agile under configuration control for comparison and analysis.

The contractor shall complete system integration testing and user acceptance testing in the pre-production environment and shall work with the FNS OIT to provide source code; software build scripts and installation instructions; associated design, development, and testing artifacts; and release notes prior to sprint deployments from the development environment to the pre-production environment and from the pre-production environment to the production environment for final release deployment. The contractor shall address any issues found within the <Application/System Name> software, installation procedures, documentation, or other items relevant to successful testing and deployment of a releasable software delivery. Also, outstanding defects that are discovered during the 90-day warranty period shall be addressed in a technical debt sprint at no cost to FNS OIT.

At the conclusion of each sprint, the definition of ***pre-production ready*** shall include the transfer of all code and configurations from the development environment to the pre-production environment. At the conclusion of UAT for each sprint or set of sprints and approval identified during Decision Point reviews, the definition of ***production ready*** shall include the approval of all code and configurations in the pre-production environment. At the conclusion of each release deployment and validation, the definition of ***done*** shall include the transfer of all code and configurations from the pre-production environment to the production environment and delivery of all source code to the FNS Team Foundation Server (TFS) Centralized Code Repository (CCR).

The contractor shall design, develop, and test software to meet existing and planned <Application/System Name> architecture and deployment requirements and conform to the <Application/System Name> non-functional requirements. The contractor shall comply with requirements for assessment and authorization that are required in advance of production deployment and shall conduct security scans as required by FNS OIT using government provided tools. Agile projects will require several iterations, culminating in a release to production. The size and complexity of the user stories will drive the number and length of the iterations and Release Schedule.

The contractor shall develop or edit and maintain the documentation identified in Appendix B - <Application/System Name> Project Process Agreement to reflect the changes resulting from releases:

### Pre-Deployment

Each build shall include approximately 3 to 4 sprints and shall be deployed from the development environment to the pre-production environment for System Integration Testing (SIT) and User Acceptance Testing (UAT) to ensure end-user acceptance and identify any vulnerabilities in the system. There may be one or multiple builds in a release. The facilitation of SIT and UAT in the pre-production environment allows time for the contractor to address issues and concerns raised by the testers from the contractor as well as the end-users, prior to deployment to the production environment. All defects in the system shall be remediated at the contractor’s expense. The contractor shall work with the FNS OIT COR, Product Owner, and Program Manager to determine priorities in addressing any defects prior to deployment to the production environment.

The contractor shall ensure that all delivered code is version-controlled, ensuring that configuration management (CM) process and procedures are adhered to and in place for the continued development of the system. CM shall include code control in the development, pre- production, and production, as well as backup/disaster recovery environments.

FNS OIT will, at its discretion, perform independent penetration testing on any release to ensure that the Secure Code Policy of the Department has been met. Systems that have vulnerabilities and do not meet the standards of the Secure Code Policy shall not be released to the production environment. The contractor shall test systems and applications for security vulnerabilities prior to their deployment to the pre-production environment. If a release is found to have vulnerabilities, the release shall not be allowed to proceed and the contractor shall remediate the vulnerabilities at no additional cost to the government.

The contractor shall develop or edit and maintain the documentation identified in Appendix B - <Application/System Name> Project Process Agreement to reflect the changes resulting from releases:

### Deployment

Through several steps of design, development, and testing, followed by data migration and pre- deployment, the contractor shall work with FNS OIT to implement both functional and non-functional requirements for <Application/System> in the production environment. The contractor shall ensure that all production deployments are duplicated and mirrored in a training environment for all releases. System deployments shall include releases of one or more sprints with themes focused on the system, database and infrastructure and all source code shall be free from errors as much as possible.

The contractor shall develop a working and holistic understanding and knowledge of the FNS OIT hosting environments, including those cloud hosting environments supported by the Department or another government agency. The solution shall be align with FNS Enterprise Architecture and the IT Modernization Cloud-Based solutions. The contractor shall serve as the source of technical expertise with regards to maintaining and improving <Application/System Name> in the development, pre-production, and production environments.

The contractor shall develop or edit and maintain the documentation identified in Appendix B - <Application/System Name> Project Process Agreement to reflect the changes resulting from releases:

## Transition Support

*This section is required in all PWSs.*

At the close of contract period, should work transfer to another contractor, the contractor shall prepare project artifacts and provide knowledge transition in a manner that reduces risk to the maximum extent possible. The contractor shall compile lists of roles, responsibilities, POCs, file and code repositories, documentation sources, application status, open project risks, help desk tickets, and other in-progress tasks. The contractor shall ensure the latest source code version is stored in the FNS Enterprise TFS CCR and provide reconciliation evidence to FNS. The contractor shall review their Transition Out plan with the COR and be prepared to execute this plan upon notification of contract transition by the Contracting Officer (CO). The contractor shall conduct a project transition knowledge transfer kick-off session with the incoming contractor, agreeing upon items necessary to ensure a seamless transition that reduces risk to the <Application/System Name> application/program.

FNS may need to transfer this platform to another contractor or service provider. The contractor shall not create the platform in a manner that imposes obstacles to such transfers, nor hold the data hostage to a proprietary software, service, or hardware. The scope of this contract includes any activities to facilitate the transition of the platform to a different contractor or service provider.

## Miscellaneous Task Examples

*The following subsections are examples for additional tasks for inclusion into your PWS and should be tailored to address project specific requirements. Rename and renumber Headings as necessary.*

### Sustainment

*The following subsections are examples for Sustainment activities (O&M).*

The following subsections describe the Sustainment activities for the <Application/System Name> application.

#### Data Handling and Validation

The contractor shall perform the function of receiving, loading, validating, storing, and archiving the data obtained from <the source>. The <Application/System Name> system will use the output from the data validation for further analysis. Tasks included as part of data validation include: (a) cleaning data, (b) running data validation tests, (c) identifying data anomalies indicative of errant authorization numbers, duplicate records, using standard analysis techniques to identify data that is most likely to be erroneous, such as an unusual number of client transactions from a distant state, (d) Identifying daily spike indicators of ramped up trafficking in the incoming data obtained from the <the source>, and (e) monitoring terminal activity when requested.

#### Data Management

The contractor shall work with FNS’ OIT to establish and manage a data management process for the system. FNS defines data management as all activities related to managing data used in the system. This includes acquiring, validating, storing, protecting, and processing the data. For PII data, FNS requires the use of encryption and security measures consistent with the standards established by the National Institute of Standards and Technology in accordance with NIST Special Publication 800-122 (see Appendix E).

#### Database Support

The contractor shall perform the function of Database Administration in support of the <Application/System Name> application. Database Administration includes tasks performed on a regular basis to monitor and maintain the health of the databases and database server environments, and includes performing necessary database tune-ups, executing all automated jobs successfully as scheduled and supporting maintenance release development activities. Tasks for the DBA are: (a) assistance with the installation, configuration and upgrading of Microsoft (MS) Structured Query Language (SQL) Server software and related products, (b) database design, development and assistance with implementation, (c) establish and maintain backup and recovery policies and procedures, (d) implement and maintain database security (create and maintain users and roles, assign privileges), (e) perform database tuning and performance monitoring, (f) perform application tuning and performance monitoring, (g) set up and maintain database documentation and standards, (h) plan growth and changes (capacity planning), (i) work as part of a team and provide occasional off-hours support when required, and (j) perform general technical trouble-shooting and give consultation to development teams. There could also be other tasks assigned to the DBA on an as-needed basis.

The contractor shall provide support for the maintenance of the production environment for any production element of the <Application/System Name> application. Operations shall include running operational components designed for administrators and/or operators, monitoring the operational integrity of systems during operation cycles, communicating with external organizations and the user community and tracking activities performed via logs, status reports, and available statistical information and analysis.

Production Support also includes tasks performed on a regular basis to monitor and maintain the health of the <Application/System Name> application and application server environments, as well as installation of software patches, researching and resolving Help Desk issues, implementing emergency fixes and working on maintenance release development activities (requirements, design, development, testing, and deployment). It also includes tasks to make sure each system release complies with USDA security guidelines and web standards and assisting FNS with any A&A process tasks for <Application/System Name> as and when appropriate. Note: The contractor does not perform the A&A itself.

#### Deployment

The contractor shall deploy each release (fixes, etc.) to the testing environments (INTEG and UAT) and conduct testing to ensure all code works as expected. The contractor shall facilitate UAT in the UAT environment with sufficient time for the contractor to address issues and concerns raised <Application/System Name> end-users prior to deployment to the pre-production and production environments. All high priority vulnerabilities in the application shall be remediated at the contractor’s expense. Emergency releases, which include software upgrades, system patches, bug fixes and updates to reflect business changes are required on occasion but kept to a minimum.

The contractor shall deliver software code for every vulnerability remediated digitally signed release to include executables, scripts, source code, configuration files, test scripts, and any COTS products with associated license keys and documentation to the FNS Enterprise TFS CCR.

*Include this paragraph if applicable.* The contractor shall also deploy each release to the training environment and ensure that the training environment is available and accessible to end users for monthly training sessions. The contractor shall also provide support to backup and restore the training database as needed to support the monthly training sessions

All web pages must be in compliance with Section 508 standards. The contractor shall conduct testing to ensure the <Application/System Name> application is in compliance with Section 508 standards and best practices, as determined by FNS OIT in accordance with Department standards.

The contractor shall ensure that all delivered code is version-controlled. Coding support will include ensuring that configuration management (CM) process and procedures are adhered to and in place for the continued development of the system. CM will include code control in the development, pre-production, and production, as well as backup/disaster recovery environments and any additional environment existing or new. All source code delivered, both compiled and uncompiled, must be placed into the FNS Enterprise TFS CCR.

The government will, at its discretion, perform independent penetration testing on any release to ensure that the Secure Code Policy of the Department has been met. Applications or systems that have vulnerabilities and do not meet the standards of the Secure Code Policy will not be released to the production environment. It is the responsibility of the contractor to test systems and applications for security vulnerabilities prior to their delivery to the Agency. If the application or system of a release is found to have vulnerabilities the release will not be allowed to proceed and the contractor shall remediate the vulnerabilities at no additional cost to the government.

The contractor shall provide post-deployment support for the releases as part of normal <Application/System Name> Sustainment responsibilities and subject to the SLA and the Blanket Purchase Agreement (BPA). The contractor shall provide ongoing support as is provided for normal <Application/System Name> software releases and system level operations.

#### Disaster Recovery Site Maintenance and Simulations

Disaster Recovery (DR) site(s), which can be used in the event of a catastrophic failure in Production, is vital. Disaster recovery database servers are regularly updated with the latest production backups and data, following well defined and documented procedures. Disaster recovery drills are performed periodically to ensure daily production data is readily available to be restored.

#### Secure Configuration and Application and Operating System Patches

The contractor shall ensure that the system, once operational, is properly maintained and monitored, to include immediate response to critical security patches, implementation of required security patches and updates, and compliance with the defined secure configuration requirements for all IT components associated with the solution:

| **Vulnerability Category** | **Response** |
| --- | --- |
| Critical Vulnerabilities | Applied within 2-weeks |
| High Vulnerabilities | Applied within 30-days |
| Medium Vulnerabilities | Applied within 60-days |
| Low Vulnerabilities | Applied within 180-days |

Table 3 - Vulnerability Response Time

### System Monitoring and Support

The contractor shall provide adequate support for the operations of <Application/System Name> in the development, training/UAT/pre-production, and production environments. Operations includes running operational components designed for system administrators, monitoring and maintaining the operational integrity of the system, configuration management, production database updates, patching, bug tracking and resolution, communicating with external organization, and tracking activities performed through logs, status reports, matrices, and available statistical information and analysis. Where necessary, the contractor shall work with representatives for one or more support groups (e.g. OIT, ISO, Digital Infrastructure Services Center (DISC), Client Experience Center (CEC), Users, Front-end issues, Back-end issues, etc.).

The contractor, in close collaboration with FNS OIT, shall ensure timeliness and availability in order to support end-users in their business process and produce minimal impact during business hours.

The contractor shall be responsible for support in identifying and troubleshooting problems as they occur, internally and externally of who is responsible for the root cause risk or production issue.

The contractor shall develop, for the COR approval, a Service Level Agreement (SLA) that details the support levels, personnel, hours of operation, sprint velocity, response times, conditions, and expectations for supporting <Application/System Name>. The SLA shall be submitted to OIT NLT 30 days after contract award. At a minimum, the SLA shall provide:

* Average monthly velocity
* Documented process and workflow
* Reporting capabilities that include flexibility and data elements which can be customized.
* Support from least technical to highest technical.
* Assurance that enhancements and defects are corrected in agreement with the priorities established by FNS.
* Use of a government-provided performance monitoring tool to ensure system uptime requirements are met.
* Reporting leaks or data breaches following FNS process and procedures.

The SLA identifies the government management processes that the contractor shall support, along with procedures and time constraints for situations in which the application or system is not responding normally.

The contractor, in close collaboration with FNS OIT, shall develop and deliver a checklist identifying the features of the <Application/System Name> project that will be verified for operational readiness. The checklist shall include elements ensuring that the system is responding normally, the database is correctly responding, and the back-up procedures are executed correctly. The contractor shall review the elements of the checklist within the development, pre-production and production environments, as well as a training environment. The checklist shall be reviewed and delivered quarterly to identify any elements to be included, deleted, or changed.

### Data Mining

The contractor shall provide the expertise and support for data modeling and analysis on data provided by FNS within the framework of the existing system.

Specific data mining needs include:

* Analyzing historic data and analytic outcomes of actual case results to assess the effectiveness of specific scan and analytic methods already in use.
* Developing new analytic tools with collaboration and input from key FNS SMEs.
* Exploring and analyzing known and unknown fraud scenarios.
* Creating behavior patterns in terms of store and household transaction attributes as defined by FNS experts.
* Performing hypotheses testing and modeling.
* Providing products to incorporate into the system.
* Introducing new data sets approved by FNS to enhance system capabilities.
* Explore new data modeling and analytical techniques to help identify and strengthen prediction patterns.

The contractor will work closely in collaboration with FNS key staff on data mining activities for input and validation. System users may provide input in the various stages as SMEs to ask some of the questions.

The contractor will analyze and validate existing analytical tools and reports, risk profiles, and other established tools to assess their validity and determine whether refinements are necessary. The contractor shall analyze and validate any new models and/or scans introduced as part of this project. Such an analysis will be an ongoing effort (at least annually) and not a one-time event.

Data mining activities will occur on an ongoing basis in the FNS data mining database.

### Help Desk

The contractor shall receive, track, resolve, and report on <Application/System Name> Help Desk inquiries. The contractor shall provide Help Desk operation for all active or potential users of the <Application/System Name> application. During the Calendar Year 20<XX>, there were <XX,XXX> requests to the <Application/System Name> Help Desk.

#### Service Availability

The help desk will be staffed from 8:00 AM to 6:00 PM Eastern Time each Business Day. A “Business Day” is Monday through Friday, excluding Federal holidays and when the Federal government offices are closed. Voice mail that is regularly checked is acceptable for managing phone messages. The Help Desk will be available for the duration of the contract period of performance.

#### Standard Help Desk Services

The contractor shall provide the following standard help desk services:

* Provide Help Desk staff, knowledgeable in <Application/System Name>, and be able to respond to questions ranging from Web browser configuration and software configuration to <Application/System Name> application use. This is a Tier 1 service.
* Escalate an unresolved inquiry over 24-hours to Tier 2 within one business day and notify the user. Tier 2 Service will require a fix from the development or database analysis support or from a government <Application/System Name> SME.
* Inform the users of the status of their inquiry as it progresses through the resolution process. Provide updates every 48-hours or upon a status change, whichever time period is less.
* Log all Help Desk inquiries into Jira, FNS’ system of record for <Application/System Name> tickets and collect the following information: description of the problem, date, and time of ticket initiation, severity of the reported problem, and names of the parties involved. The contractor will make this information available in a report format to FNS as requested but no less frequently than weekly (embedded in weekly report).
* Review aged (older than 2-weeks) Help Desk tickets on a bi-weekly basis. At a minimum, the analyst supporting the Help Desk attends this meeting. The Help Desk analyst distributes action items to resolve aged tickets to the participants within 24-hours of the meeting.
* The contractor shall provide ongoing feedback regarding user issues that could be resolved with future enhancements. The contractor team shall regularly review and analyze Help Desk activity to identify potential risks to any affected systems.
* Track and monitor all problems to closure.
* Enter all problems/user requests that may result in a system modification as Change Enhancement Requests (CERs) in Jira.
* Complete approved data requests for archived data and deliver the data in an approved secure manner to the requestor. The <Application/System Name> Help Desk received <XX> data requests during 20<XX>. Maintain a record of requests and deliveries for three years. Specialized, occasional queries of the <Application/System Name> system will be supported for research purposes subject to COR approval and contractor agreement that the request is within the scope of the contract.
* The contractor shall develop and maintain a Help Desk Guide that includes work instructions for administering the Help Desk duties and <Application/System Name> FAQs based on common requests from past 12-months. The contractor must proactively update the Help Desk guide and user FAQs, with quarterly updates expected at a minimum. The guide should also include instructions to manage the telephone, voicemail, and email.
* Establish and control user accounts according to USDA/FNS Security policies and include instructions for account administration within the Help Desk Guide.
* Handle queries not related to <Application/System Name> with professional and customer friendly responses in keeping with the USDA objective of being customer focused. Develop a concise list of responses to inquiries to best address calls and messages intended for other USDA or SNAP projects and maintained within the <Application/System Name> Help Desk Guide.
* FNS will provide a dedicated telephone line and a support desk email address.

#### Telephone Line and Voicemail

Support desk will have one dedicated phone line to respond to the phone number supplied by FNS and access to one voicemail box.

A support desk staff will respond to incoming telephone calls and voicemails and respond as specified below:

| **Item #** | **Incoming** | **Response Window for Business Day** | **Response** |
| --- | --- | --- | --- |
| 1 | Telephone | 8:00 am to 6:00 pm | Answer calls as they come in unless with another support caller or on a government required call. |
| 2 | Voicemail | 8:00 am to 5:00 pm | Respond to message within 60 minutes, unless occupied with another caller or help desk inquiry. |
| 3 | Voicemail | After 5:00 pm but before 8:00 am | Respond by 9:00 am. |
| 4 | Voicemail | Non-business days | Respond by 9:00 am next business day. |

Table 4 – Telephone Line and Voice Response Times

#### Email

A support desk staff will respond to emails as they come in and respond to messages as specified below:

| **Item #** | **Incoming** | **Response Window for Business Day** | **Response** |
| --- | --- | --- | --- |
| 1 | Email | Up to 5:00 pm | Respond to messages within 60 minutes |
| 2 | Email | Beyond 5:00 pm | Respond to messages before 9:00 am next business day |

Table 5 – Email Response Times

### Database Administrator Activities

The contractor will perform any DBA activities, such as schema changes, required to complete the coding of the releases.

The deliverables from the System Development tasks will be a software package for production installation and updates to existing documentation as specified in this PWS.

### Data Governance

The contractor shall work with FNS’ OIT to establish and manage a data governance process for the platform. FNS defines data governance as the rules, principles, and policies that govern managing data within the platform.

### Data Management

The contractor shall work with FNS’ OIT to establish and manage a data management process for the platform. FNS defines data management as all activities related to managing data used on this platform. This includes acquiring, validating, storing, protecting, and processing the data. For PII data, FNS requires the use of encryption and security measures consistent with the standards established by the National Institute of Standards and Technology in accordance with NIST Special Publication 800-122 (see Appendix E).

### Data Architecture

Data is constantly changing and unpredictable. Many forms of data available to FNS and its States partners today, like social media posts or third-party data matches, were not available 15, 10 or 5 years ago. FNS expects to be able to continuously evolve its practices using structured and unstructured data as it is impossible to predict what will be available in the future. The scope of this contract includes any activities to build, maintain, or enhance the data architecture to equip the platform to handle any type of data, analysis, and application in the future. The contractor shall build the database leveraging the latest technology to limit the amount of sensitive data captured and stored to mitigate security risks, and ensure availability of the data to meet annual reporting requirements.

### Production Database Change Requests

There are times in which the application or system owner may need to change the data in the database but not affect a functional or technical change, also referred to as a production database change request (PDCR). Changes in which just the data in the database is changed without adjusting the logical tier or the presentation tier are known as PDCRs.

The contractor will perform functions that require “touching” the code or data that users cannot do themselves. Examples include:

* deleting duplicate or erroneous reviews and/or associated documents, upon user request;
* running data queries to support analysis of data quality or to answer questions not addressed in existing reports;
* adding or removing user access;
* updating user roles;
* adding / updating reference tables (e.g. moving a state from one region to another; adding/deactivating/updating finding tier structures, findings and/or observations etc.).

The contractor has a responsibility to test the change or changes in the testing environments, ensure that PDCRs meets expectations, validate proper display and function within a specific list of Internet browsers for compatibility, and verify that there are no unintended impacts. The contractor will send a Test Results and Evaluation Report to the COR indicating whether the changes passed or failed testing. For any failed testing, the contractor will correct any issues and test (again) the change or changes in the testing environment and update the Test Results and Evaluation Report. Generally, they are Structured Query Language (SQL) statements that insert, delete, or change one or more data points to meet the needs of the Product/Business Owner and end-users.

The contractor will deliver the code to be executed. The contractor also will deliver metrics indicating the number of records impacted as well as a test script to verify that the data has been changed.

For each PDCR, the contractor will work with the COR and Product/Business Owner, as well as end-users, to establish requirement(s) reviews and communications regarding the schedule and final results of pre-production and production releases. Before deploying a PDCR in the pre-production and production environments, the contractor also will work with the COR to provide a short description of the PDCR, required downtime and affected servers. Finally, the contractor shall deliver a document that briefly identifies the changes or adjustments to the database in the form of Release Notes. Release Notes should be user-friendly, non-technical, and easy to understand for the end-user community for all changes.

The PDCR also will be tracked as a discrete type of change request / release during Weekly Status Meetings.

### Configuration Releases (Patching)

Throughout the period of performance, the application or system owner may need to make Configuration Releases to the application/database server. These types of changes may result from the issuance of a patch from a software vendor, e.g. Microsoft Patch. These types of changes may also result from the issuance of a Security Bulletin from organizations like the US Computer Emergency Readiness Team (US CERT), the Department Office of Cyber Security (Cyber) FNS’s Technology Division Change Control Board (CCB), or even from FNS’s Information Security Office (ISO). In all instances there is a time component for implementing the change and the potential introduction of a vulnerability if the change is not implemented. The contractor shall assist CEC and/or DISC with monthly patching (or as needed) and validate that the <Application/System Name> application and reports are online before the start of the next business day (8am EST) after patching. Patches are usually conducted by CEC and/or DISC on weekends and usually only require the vendor to validate and report the status after patching before 08:00 Eastern time on Mondays.

The contactor shall be responsible for proactively requesting and reviewing system vulnerability reports for all <Application/System Name> environments and servers on a weekly or bi-weekly basis. The contractor shall provide remediation recommendations for system vulnerabilities as well as software upgrades to remain current. The contractor shall be responsible for applying approved updates and patches for all software above the operating system level on a regular ongoing basis to mitigate system vulnerabilities and remain on supported software for all third-party software utilized in the <Application/System Name> application.

These types of changes will be accounted for in the third number set for an application’s release. For example, if this is the third Configuration Release under minor release 2.2, then the application will be labeled as 2.2.3. When possible, a Configuration Release may be combined with a scheduled minor release, PDCR and/or major release. The contractor has a responsibility to test the change or changes in the pre-production environment, validate proper display and function within a specific list of Internet browsers for compatibility, and verify that there are no unintended impacts. In these instances, a separate party, responsible for infrastructure, will deploy the Configuration Change(s) to the non-production environment. The contractor will review the scope of the Configuration Release and test the system or application to verify that there is no negative impact to the application or system from the change. The contractor will send a Test Results and Evaluation Report to the COR indicating whether the changes passed or failed on the regression test. For any failed testing, the contractor will correct any issues and test (again) the change or changes in the pre-production environment and update the Test Results and Evaluation Report.

In the event that there is a patch or configuration release that has a negative impact to the performance or operation of the application the contractor will alert the COR and Product/Business Owner and identify a course of action to implement a change to the application that will allow the patch or adjusted configuration to be applied. That change will be added as a Change Enhancement Request and will be included in the next regularly scheduled release.

FNS and USDA will run regular vulnerability scans on all applications at least on a weekly basis. The contractor shall remediate vulnerabilities according to the FNS Vulnerability Response Criteria.

# SECTION 508 – ACCESSIBILITY OF INFORMATION AND COMMUNICATIONS TECHNOLOGY

*This section is a requirement and contains standard language for all projects. Ensure that you complete the Acquisition Request Tool in last section - ICT Accessibility Requirements Statement per the Revised Section 508 of the Rehabilitation Act and paste the results into the subsection.*

1. This PWS 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 (PL 105-220). Specifically, subsection 508(a)(1) requires that when the Federal Government procures Information and Communications Technology (ICT)[[1]](#footnote-2), 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.
2. The ICT accessibility standards as 36 Code of Federal Request (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.
3. 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 CO determines any furnished product or service is not in compliance with the contract, the CO 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 Government in writing. If such repair or replacement is not completed within the time specified, the Government shall have the following recourses:
4. Cancellation of the contract, delivery, or task order, purchase or line item without termination liabilities; or
5. In the case development of custom Information and Communications Technology (ICT) 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.
6. The contractor shall provide all ICT products and services that are less than fully compliant with the accessibility standards pursuant to extensive market research and are the most current compliant products or services available to satisfy the contract requirements.
7. 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.

## Section 508 Accessibility Standards

The <Application/System Name> shall comply with the standards, policies, and procedures below. In the event of conflicts between the referenced documents and this PWS, the PWS shall take precedence.

1. 29 U.S. Code (U.S.C.) 794d (Rehabilitation Act as amended)
2. 36 CFR 1194 (Section 508 standards)
3. [Section 508 standards by Access Board link](https://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards/section-508-standards)
4. FAR 39.2 (Section 508)
5. [USDA Departmental Regulation 4030-001 link](https://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 subcontractors) 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 PWS shall be the responsibility of the contractor or consultant.

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

* 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

### Software Development, Software Applications and Operating Systems

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

For **software development, software applications, and operating systems** the contractor shall comply with the following standards, policies, and procedures:

1. 29 U.S.C. 794d (Rehabilitation Act as amended)
2. 36 CFR 1194 (Section 508 standards)
3. 36 CFR Part 1194.21 provisions a-l
4. 36 CFR Part 1194.31 provisions a-f
5. 36 CFR Part 1194.41 provisions a-c

### Web-based Applications

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

1. 29 U.S.C. 794d (Rehabilitation Act as amended)
2. 36 CFR 1194 (Section 508 standards)
3. 36 CFR Part 1194.21 provisions a-l
4. 36 CFR Part 1194.22 provisions a-p
5. 36 CFR Part 1194.31 provisions a-f
6. 36 CFR Part 1194.41 provisions a-c

### Telecommunication Products and Services

For **telecommunication** products and services the contractor shall comply with the following standards, policies, and procedures:

1. 29 U.S.C. 794d (Rehabilitation Act as amended)
2. 36 CFR 1194 (Section 508 standards)
3. 36 CFR Part 1194.23 provisions a-k
4. 36 CFR Part 1194.31 provisions a-f
5. 36 CFR Part 1194.41 provisions a-c

### Video and Multimedia Applications

For **video and multimedia applications** (including training materials), the contractor shall comply with the following standards, policies, and procedures:

1. 29 U.S.C. 794d (Rehabilitation Act as amended)
2. 36 CFR 1194 (Section 508 standards)
3. 36 CFR Part 1194.24 provisions a-e
4. 36 CFR Part 1194.31 provisions a-f
5. 36 CFR Part 1194.41 provisions a-c

### Self-Contained and Closed Products

For **self-contained and closed products**, the contractor shall comply with the following standards, policies, and procedures:

1. 29 U.S.C. 794d (Rehabilitation Act as amended)
2. 36 CFR 1194 (Section 508 standards)
3. 36 CFR Part 1194.21 provisions a-l
4. 36 CFR Part 1194.25 provisions a-j
5. 36 CFR Part 1194.31 provisions a-f
6. 36 CFR Part 1194.41 provisions a-c

### Desktop and Portable Computers

For **desktop and portable computers**, the contractor shall comply with the following standards, policies, and procedures:

1. 29 U.S.C. 794d (Rehabilitation Act as amended)
2. 36 CFR 1194 (Section 508 standards)
3. 36 CFR Part 1194.21 provisions a-l
4. 36 CFR Part 1194.26 provisions a-d
5. 36 CFR Part 1194.31 provisions a-f
6. 36 CFR Part 1194.41 provisions a-c

### Help Desk and Other Support Services

For **help desk and other support services**, the contractor shall comply with the following standards, policies, and procedures:

1. 29 U.S.C. 794d (Rehabilitation Act as amended)
2. 36 CFR 1194 (Section 508 standards)
3. 36 CFR Part 1194.31 provisions a-f
4. 36 CFR Part 1194.41 provisions a-c

If the help desk or other support services include **training**, the contractor 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:

1. 36 CFR Part 1194.21 provisions a-l (installable and web-based training)
2. 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. A Federal Section 508 Testing Center must administer this test.

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.

### WCAG 2.0 Compliance

*This section is a requirement and contains standard language for all projects.*

The <Application/System Name> shall comply with the standards, policies, and procedures below. In the event of conflicts between the referenced documents and this PWS, the PWS shall take precedence.

#### Custom ICT Development Services

When contractor provides custom ICT development services pursuant to this contract, contractor 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 contractor provides installation, configuration, or integration services for equipment and software pursuant to this contract, the contractor 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

The contractor 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

The contractor 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, the contractor 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 contractor 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, the contractor 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

The contractor 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, the contractor shall provide an Accessibility Conformance Report (ACR) for each ICT item developed, updated, and configured for the agency, and for offered product substitutions. The contractor shall base the ACR on the latest version of the [Voluntary Product Accessibility Template (VPAT)](https://www.section508.gov/sell/vpat) provided by the [Information Technology Industry (ITI) Council](http://www.itic.org/policy/accessibility). For award consideration, the contractor shall submit an ACR for each ICT item according to the instructions provided by ITI.

When the contractor is required to perform testing to validate conformance to the agency’s accessibility requirements, the contractor 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 inaccessible 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, FNS 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

*This section is a requirement and contains standard language for all projects.*

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

## ICT Accessibility Requirements Statement per the Revised Section 508 of the Rehabilitation Act

*This section is a requirement for all projects. Complete the* [Accessibility Requirements Tool](https://buyaccessible.gov/) *(ART) for the new or existing procurement. Copy the specific language generated from the ART form into this section. Refer to the* [ART User Manual](https://buyaccessible.gov/art-user-guide) *for detailed instruction on completing the ART.*

<Paste Here>

# INTELLECTUAL PROPERTY AND KNOWLEDGE TRANSFER

*This section is a requirement and contains standard language for all projects.*

It is the intent of FNS to preserve the knowledge that the contractor amasses over the duration of the project. Throughout the duration of the contract, the contractor shall ensure that FNS does not lose this valuable information and data. FNS maintains a dedicated data repository (i.e., PartnerWeb, SharePoint, etc.) to house relevant system information and ensure ongoing knowledge management and transfer.

The contractor shall not utilize any proprietary solution that limits the government’s flexibility to change contractors and shall not house data using proprietary software. In the event that contractor’s system contains any proprietary elements, the contractor agrees to grant FNS a nonexclusive and nontransferable license to use such software at no additional cost to FNS.

## Knowledge Transfer

Subject to any qualification or provision to the contrary in this PWS, the contractor must provide the following assistance to FNS during and upon termination or expiration of this task order:

1. Providing the data elements identified in the Portfolio Management Division (PMD) data repository.
2. Providing all code related to data mining, data analytics, predictive modelling, database queries, or any data/analysis-related other task performed for this contract.
3. Transferring or providing access to all information produced while performing work on each task order issued under this PWS or requested by the COR.
4. Making contractor personnel available for discussions with the COR or designated technical personnel as required to ensure the transfer of such information - the time, length and subject of which will be at the sole discretion of the COR and designated technical staff.

## Recording and Disclosure of Contract Intellectual Property

Upon task order award, the contractor shall at all times maintain full, true, and up-to-date accounts of all intellectual property (IP) specific to this Contract. IP may include, but is not limited to:

1. Inventions
2. Software
3. Databases
4. Lessons learned
5. Documentation
6. Training materials and/or tools
7. Source code
8. Processes
9. Jointly Developed Methodologies
10. Other IP as identified in the PWS

## Cooperation with other Service Providers

From time to time, contractor may need to cooperate with third party service provider, as directed by the CO/COR, in order to ensure the integrated and efficient performance of the Customer's projects and operations. The contractor must provide such reasonable assistance to other service providers as required under the task order PWS or requested by the CO/COR within the scope of this PWS.

## Email

*This section is optional.*

Contractor staff are expected to use USDA email as the sole means of transmitting FNS proprietary information, upon receipt of a provisioned account. This includes the forwarding email to non-governmental email accounts. Until that time, contractor staff must use a company provided email account. Use of Gmail, AOL, Yahoo, or other public email domains is prohibited.

# APPLICABLE DIRECTIVES

*This section is a requirement and contains standard language for all projects. Check links to ensure it still works, and updated as needed.*

## Industry Standards

The contractor shall have knowledge in and be able to comply with prevailing standards, regulations, and guidelines, applicable to software development, including but not limited to:

1. Information Technology Infrastructure Library (ITIL) – [Link to ITIL official website](http://www.itil-officialsite.com/).
2. Control Objectives for Information and Related Technology (COBIT) [Link to ISACA COBIT webpage](http://www.isaca.org/cobit.htm).
3. Institute of Electrical and Electronics Engineers (IEEE) 1012-2016, IEEE Standard for System, Software, and Hardware Verification and Validation - [Link to IEEE 1012-2016](https://ieeexplore.ieee.org/document/8055462).
4. Software Engineering Institute (SEI), Introduction to Software Verification and Validation, Curriculum Module SEI-CM-13-1.1, 1988 - [Link to SEI-CMM Software Verification and Validation Curriculum Module](https://resources.sei.cmu.edu/asset_files/CurriculumModule/1988_007_001_15695.pdf).
5. Institute of Electrical and Electronics Engineers (IEEE) 29148-2018 - ISO/IEC/IEEE International Standard - Systems and software engineering -- Life cycle processes -- Requirements engineering. [Link to IEEE 291489-2018](https://standards.ieee.org/standard/29148-2018.html).
6. Institute of Electrical and Electronics Engineers (IEEE) 16326-2019 ISO/IEC/IEEE International Standard - Systems and software engineering - Life cycle processes - Project management. [Link to IEEE 16326-2019](https://standards.ieee.org/standard/16326-2019.html).
7. Institute of Electrical and Electronics Engineers (IEEE) 14764-2006 - ISO/IEC/IEEE International Standard for Software Engineering - Software Life Cycle Processes – Maintenance [Link to Standard 14764-2006](https://standards.ieee.org/standard/14764-2006.html).
8. Institute of Electrical and Electronics Engineers (IEEE) 26511-2018 - ISO/IEC/IEEE International Standard - Systems and software engineering - Requirements for managers of information for users of systems, software, and services [Link to Standard 26511-2018](https://standards.ieee.org/standard/26511-2018.html).

Furthermore, the contractor shall establish policies, processes, procedures, and metrics that will ensure the outputs meet contract requirements and facilitate continuous improvement of products and processes.

Desirable certifications include, but are not limited to:

1. Capability Maturity Model Integration (CMMI) Level II or above through the life cycle of the contract [Link to CMMI Institute](https://cmmiinstitute.com/cmmi).
2. International Organization for Standardization (ISO) 9001:2015 certified [Link to ISO 9001:20015](https://www.iso.org/standard/62085.html).

## Other Federal Government and USDA Requirements

The contractor shall comply with these standards, as applicable, and include but are not limited to:

1. Federal Enterprise Architecture
2. Privacy Act of 1974
3. NIST Special Publication 800-37, Revision 2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy (December 2018), [Link to NIST Publication 800-37, Rev2](https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final).
4. United States Department of Agriculture (USDA) Food and Nutrition Service (FNS), Agile Systems Development Lifecycle (SDLC) Guide, Version 1.0, *pending release*. Refer to Appendices
5. United States Department of Agriculture (USDA) Certification and Accreditation Guide, Version 4, (March 2005), [Link to USDA Certification and Accreditation Guide](https://www.ocio.usda.gov/sites/default/files/docs/2012/DM3555-001.pdf).
6. Section 508 of the Rehabilitation Act of 1973, as amended (29 U.S.C. 794d) for system accessibility requirements, [Link to Section 508 of the Rehabilitation Act of 1973 via Access Board.](https://www.access-board.gov/the-board/laws/rehabilitation-act-of-1973)
7. System of Record Notice (SORN) USDA/FNS-10, entitled Persons Doing Business with the Food and Nutrition Service March 31, 2000 (Volume 65, Number 63)] [Pages 17251-17252]
8. The contractor shall develop and implement an innovative technical solution that ensures compliance with all applicable federal IT standards and security standards. The contractor shall provide IT security development support for configuration management, change request process, and the evaluation of technical designs during the engineering process.
9. The contractor shall apply all relevant operating system and application security technical implementation guides (STIGs).
10. Department of Homeland Security (DHS) Binding Operational Directives, Appendix F, directing required action on the part of certain federal agencies in the civilian Executive Branch, [Link to DHS Binding Operational Directives webpage](https://cyber.dhs.gov/directives/).

## Compliance with Internet Protocol Version 6 (IPv6)

(a) Any system, hardware, software, firmware or networked component (voice, video or data) developed, maintained, 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:

(b) Specifically, any IP product or system developed, maintained, acquired, or produced must:

(1) Interoperate with both IPv6 and IPv4 systems and products, and

(2) Have available contractor/FDE IPv6 technical support for development and implementation and fielded product management.

(c) 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.

(d) The contractor shall provide technical support for both IPv4 and IPv6.

(e) Any system or software must be able to operate on networks supporting IPv4, IPv6 or one that supports both.

(f) 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.

# PERIOD OF PERFORMANCE

*This section is required. Adjust the period of performance as needed.*

The base period of performance is for 12 months from contract award with one, six-month option.

# KEY PERSONNEL REQUIREMENTS

*This section is required. Adjust the key personnel and tailor experience requirements as needed.*

The contractor shall staff the project with personnel capable of successfully planning and executing the requirements and tasks outlined in this PWS. Below is a list of the minimum key personnel; however, the contractor may propose additional personnel as they see fit to meet the requirements in the PWS. Whereas all contract personnel working on the project for greater than 120 days must undergo a federal background investigation, the positions listed below must additionally have an active moderate risk background investigation (MBI).

At a minimum, a Project Manager must be identified and designated as Key Personnel. There may be more than one Project Manager. The Project Manager will be a direct liaison to FNS Office of Government Contracting and Business Development. The Project Manager must be a senior staff member and is responsible for the supervision and management of the contractor’s personnel, technical assistance, and interface and compliance with instructions from FNS COR.

The contractor shall propose appropriate labor categories for these positions. Outlined in the following subsections are the minimum Qualifications for Key Personnel.

*This portion is optional.*

The following requirements related to personnel must be met:

* The contractor shall assign individuals whose résumés are submitted with its proposal and who are identified in the contractor’s proposal as Key Personnel. Not all contractor employees assigned to perform this contract will be Key Personnel. The contractor shall submit résumés (as a Microsoft word document) as part of its proposal submission.
* If an individual proposed as Key Personnel becomes unavailable during the course of the source selection process, the Offeror will notify the CO immediately and provide a substitute and their résumé. The proposal of any Key Personnel not currently employed by the Offeror shall be accompanied by letters of intent signed by the proposed Key Personnel indicating their intent to be employed by the Offeror.
* The contractor agrees that during the first six (6) months of contract performance, no Key Personnel substitutions will be made unless necessitated by an individual’s sudden illness, death, or termination of employment. In any of these events, the contractor shall promptly notify the CO and provide the information required by paragraph (e) below on the proposed replacement for Government approval. No substitutions of Key Personnel shall be made except in accordance with this provision.
* After the initial six months of performance, the contractor must obtain Government approval of any substitution of Key Personnel prior to removing the approved Key Personnel from performance. All proposed substitutions/additions must be submitted, in writing, to the Contracting Officer at least 30 days (60 days if security clearances are involved) in advance of the proposed substitution and provide the information required by paragraph (e) below.
* All requests for substitutions/additions of Key Personnel must include a detailed explanation of the circumstances necessitating the proposed substitution or addition, a complete résumé for the proposed substitute or addition including skills, experience, education, training, and security level. As determined by the CO, all proposed substitutes/additions must have qualifications that meet or exceed the qualifications of the person to be replaced.
* The CO or his/her authorized representatives will evaluate the request(s) for substitutions/additions of Key Personnel and the CO will notify the contractor, in writing, of approval or disapproval. Disapproval of the proposed individual(s) shall not provide grounds for nonperformance by the contractor or form the basis of any claim for monies, delivery schedule extension, or any other equitable adjustment.
* The personnel set forth below as proposed by the contractor for this effort, or identified in the contractor’s proposal as Key Personnel, shall comprise the list of Key Personnel required to perform under this effort. The list may be modified in accordance with the above, to substitute or add personnel:

*Select appropriate key personnel for your project. The following subsections are recommended minimum qualifications for several positions. Note: Some would not be considered key personnel.*

## Senior Project Manager

* Bachelor’s degree in computer- or business-related discipline required (Master’s degree preferred).
* Minimum of ten (10) years of IT project management experience in software development or design.
* Minimum of six (6) years of experience in a supervisory capacity.
* Proven ability to complete projects on time and within the stated budget.
* Excellent communication, organization, time-management and leadership skills
* A Project Management Professional certification, Certified Scrum Practitioner (CSP) or Project Management Institute’s Agile Certified Practitioner (PMI-ACP), or a certified and experienced Scrum Master is required.
* Minimum of seven (7) years of communication experience - facilitating meetings and presentations and writing project documentation.

## Senior System Architect/Technical Lead

* Bachelor’s degree in computer- or business-related discipline required.
* Minimum ten (10) years’ experience in defining and creating software architectures and designs.
* Intensive and progressive experience developing and designing applications with the following technologies: Apache Struts2 framework, JQuery JavaScript, Alfresco services, MS SQL Server, Red Hat Enterprise Linux, Wildfly Application Server, Java Development Kit, Apache HTTP Server, and SiteMinder Web Agent.
* Demonstrated experience leading technical development efforts.
* Expert written and verbal communication skills.
* Possession of certification in related field a plus.

## Senior Database Administrator

* Bachelor’s degree in computer science, management information systems, or similar computer-related discipline required.
* Minimum of ten (10) years of experience as a database administrator, at least 5 working with data warehouses.
* Intensive and progressive experience with MS SQL Server.
* Development tasks will require intensive and progressive database design and implementation experience.
* Intensive and progressive experience with: capacity planning, installation, configuration, database design, migration, performance monitoring, security, troubleshooting, as well as backup and data recovery.
* Possession of Certified Database Administrator certificate, or similar certification.

## Senior Production Support Lead/Data Analyst

* Bachelor’s degree in computer- or business-related discipline required.
* Minimum of eight (8) years of data analytics experience and managing production support operations.
* Proven experience aligning organizational goals and priorities to activities and approaches using data tools and data management methodologies.
* Strong verbal and written communication skills.
* Expertise and experience developing and applying analytic methodologies and principles
* Demonstrated experience leading the application of analytic techniques to resolve complex problems and help define project objectives and strategic direction.
* Proficiency with the use of R services and MS SQL, and Jira.
* Troubleshoots users’ problems by analyzing information provided by users.
* Possession of certification in related field a plus.

## Senior Developer

* Bachelor’s degree in computer science, information technology, or computer-related discipline required.
* Minimum of ten (10) years of experience in programming field.
* Strong knowledge and proficiency of computer languages such as Java, PHP, and SQL 3 <insert other languages and coding items>.
* A minimum of four (4) years of communication experience facilitating meetings and presentations and writing project documentation.
* Strong background in coding and knowledge of user interfaces.
* Strong knowledge of HTML technologies and web frameworks.
* Experience developing with Java, JSP, Struts, MS SQL, JQuery, and Bootstrap.
* Experience with Jira, Red Hat Enterprise Linux, Wildfly Application Server, Apache HTTP Server, and SiteMinder Web Agent.
* Possession of certification in related programming fields a plus.

## Senior Business Analyst

* Bachelor’s degree in Business, Accounting, Information Technology, or any related field.
* Minimum of ten (10) years of related Systems Analysis and System Testing experience.
* Must be proficient in creating test cases, test case execution, documenting test results and working with programmers to resolve system findings and deficiencies.
* Minimum of five (5) years of communication experience facilitating meetings and presentations and writing project documentation.
* Must be proficient in the use of Jira.
* Intensive and progressive experience with analyzing, designing, working with developers to implement software solutions to include verification and testing.
* Experience working with clients to help define problem and make recommended solutions and coordinating with programmers on solution and production support.
* Possession of Business Analyst certification(s) a plus.

## Senior Software Developer

* Bachelor’s degree in computer science or computer-related discipline required.
* Minimum ten (10) years’ experience in design, development, and maintaining data warehouses and analytics interfaces, 5 of those years utilizing the contractor proposed solution.
* Possession of certification in related programming fields a plus.
* Certification as Application Security Specialist or Certified Information Systems Security Professional (CISSP) or industry accepted cybersecurity application certification.

## Database Administrator

* Bachelor’s degree in computer-related discipline required.
* Minimum of six (6) years of experience as a database administrator, at least 3 working with data warehouses.
* Intensive and progressive experience with MS SQL Server.
* Development tasks will require intensive and progressive database design and implementation experience.
* Intensive and progressive experience with: validating table data and repairing tables where necessary; performing analysis of databases to protect against table space exhaustion, corruption, and fragmentation; reconfiguring databases to improve performance; and ensuring data consistency and reliability in global, shared databases.
* Possession of Certified Database Administrator certificate, or similar certification, a plus.

## Database Architect

* Bachelor’s degree in computer science, information science, or similar computer-related discipline required.
* Minimum of ten (10) years of experience for Development; 5 of which include working on successful Enterprise Data Warehouse implementations.
* Intensive and progressive experience with: establishing information requirements for enterprise-wide or large scale information systems, databases, and/or networks. Design architectures that include software, hardware, and communications solutions to support the total requirements, as well as provide for present and future cross-functional requirements and interfaces.
* Possession of Certified Data Management Professional (CDMP) certificate from the Institute for Certification of Computing Professionals (ICCP), or similar certification.

# DELIVERABLES

*This section is mandatory. Required deliverables will vary based on project size and type. Documentation Submitted with the Proposal is optional and tailorable. Programmatic Deliverables are usually for development projects and are tailorable; these may also apply to Sustainment projects for maintenance purposes.*

*Continual Maintenance Deliverables are for Sustainment projects and are tailorable based on the PPA.*

High-level deliverables that adhere to the FNS SDLC Decision Point process requirements per Appendices A, B and C. All projects must pass the Decision Point process in order to proceed.

The following deliverables are required for submission by the contractor by the due date indicated or identified in writing following the contract award. The contractor must have adequate staff to complete and review all deliverables for quality prior to submission.

The contractor shall leverage the FNS tailored SDLC deliverable templates, as applicable, in order to ensure required content and level of detail are adhered to prior to submission for FNS review/acceptance. FNS SDLC deliverable templates have been included for reference in Appendix A – FNS Agile SDLC Guide and Appendix B – <Application/System Name> Project Process Agreement. The contractor shall verify with FNS and leverage the latest SDLC template prior to drafting each deliverable.

The contractor shall also fulfill the following tasks:

* Development, coordination, review, and delivery of project-related documentation and deliverables;
* Provide support in the development, coordination, review and delivery of security-related documentation and deliverables;
* Create customer-facing documentation for technical enterprise software and developer tools;
* Document complicated procedures in simple and understandable manner and compose material according to set standards and templates;
* Coordinate, facilitate, write, edit, track progress, and package documentation for review and approval among the appropriate stakeholders.

## Documentation Submitted with the Proposal

*This section is optional and tailorable.*

Prospective offerors for this work shall submit with their proposal the following documents including:

* A list of Key Personnel
* Fixed price costs for each class of service
* The Not To Exceed (NTE) ceiling Level of Effort (LOE) in terms of work hours for each class of service
* The Labor Categories and skill range (experience) of people (not necessarily “key”) proposed to perform each class of service
* Fixed price costs for each Task and optional Task
* Program Management Plan identifying:
* Project Schedule (including monthly status meetings)
* Risk Management,
* Scope Management,
* Configuration Management and
* Quality Management practices
* Monthly cost for the Program Management services

## Progress Reports, Program Reviews and Status Reports

*This is standard for all Development and Sustainment projects. Tailor based on specific project needs.*

### Progress Reports

The contractor shall provide a Monthly Progress Report that summarizes the contractor’s previous month’s activities including any management issues, status, recommendations, and suggesting resolutions. The contractor shall deliver this report by the fifth (5) business day of each month (by email transmission).

The monthly status report shall summarize the areas of the weekly reports and shall focus on the project roadmap and critical milestones approaching in the month ahead. Based on the project schedule, the contractor’s monthly status report shall include an overview of development progress, testing results, demonstrations, and lessons learned.

### Program Review

If necessary, the contractor shall hold a formal meeting to review and discuss the Monthly Progress Report no later than (NLT) the 10th business day of each month. Upon request by the OIT COR or PM to hold a Monthly Program Review Report Briefing, the contractor shall prepare the agenda, all documentation, and facilitate the discussion. Topics covered shall include but are not limited to:

1. Schedule
2. Risks/Issues
3. Scope (Change)
4. Action Items

Personnel involved in the Monthly Program Review Report Meetings shall include the COR/PM, the contractor PM, and the Product/Business Owner or designee.

### Weekly Status Reports

The contractor shall deliver (by email transmission) weekly status reports by close of business the Monday following the prior week. The COR will work with the contractor and other FNS stakeholders to determine the optimal reoccurring schedule in which the contractor shall brief the weekly status report, if applicable. Each weekly status report shall also describe the team status and any planned leave/absence that may impact the project schedule.

Personnel involved in the Weekly Status Report Meetings shall include the COR/PM, contractor PM, Product/Business Owner or designee, vendor team as appropriate, and stakeholders.

## Fully Commented Source Code Delivery

*This is standard for all Development and Sustainment projects.*

Within three (3) business days of a production software release, the contractor shall deliver to the government the fully commented source code (with explanatory notes) and final release notes which summarize code, features and functions changed, and a general description of the requirements initiating the production release. The contractor shall scan the latest release and provide required confirmation in accordance with Section 3.2.6.2 Code Review/Testing under Development Practices. This includes all source code, a comprehensive list of all tools required to compile the source code, and instructions for the use of the source code. As part of satisfying this requirement, the contractor shall utilize the VDD template from the FNS SDLC Deliverable Templates in Appendix B - <Application/System Name> Project Process Agreement. In the absence of a production software release and within 10 business days of the COR’s written request, the contractor shall also deliver the aforementioned deliverables to the FNS Enterprise TFS CCR.

## Programmatic Deliverables

*This is standard for all Development and Sustainment projects. Tailor based on specific project needs, information contained in the PWS and approved PPA.*

The contractor shall be responsible for the development and on-time delivery of the following programmatic documentation:

| **Item #** | **Deliverable** | **Section of the PWS** | **Type of Format** | **Due Date** |
| --- | --- | --- | --- | --- |
| 1 | Project Kick-Off Meeting and Draft Summary Memorandum *Standard for all projects* | Task A, Program Management & Reporting | MS Word and MS PowerPoint | Within 5 business days of contract award |
| 2 | Sprint 0 Documentation  This includes the User Stories Backlog *Typically for Development projects only; per PPA* | Task B, System Development | MS Word | Timeline to be provided and approved |
| 3 | Review Packages (Agendas, Read Ahead Packages, and Meeting Notes) *Standard for all projects.* | Task A -Program Management & Reporting | MS Word and MS PowerPoint | Phase Reviews and timing to be determined in collaboration with IT Governance Board and OIT. |
| 4 | Quarterly Release Schedule, Project Schedule/Integrated Master Schedule (IMS) *Standard for all projects; update frequency as applicable*. | Task A -Program Management & Reporting | MS Project | Timeline to be provided and approved |
| 5 | Project Management Plan (PMP) *Standard for all projects; PPA project reference artifacts.* | Task A -Program Management & Reporting | MS Word | No later than <XX> days post award and then updated as necessary. |
| 6 | Weekly Status Reports *Standard for all projects.* | Task A -Program Management & Reporting | MS Word or MS PowerPoint | Weekly – by Close of Business the Monday following the week |
| 7 | Weekly Status Report Briefing *Standard for all projects. For Sustainment projects, tailor timeframe as needed.* | Task A -Program Management & Reporting | MS PowerPoint | As Requested |
| 8 | Monthly Status Report/Management Summary *Standard for all projects.* | Task A -Program Management & Reporting | MS Word or MS PowerPoint | 5th business day of each Month |
| 9 | Monthly Status Report Briefing *Standard for all projects.* | Task A -Program Management & Reporting | MS PowerPoint | 10th business day of each Month |
| 10 | Meeting Minutes (includes Weekly Status Meetings, Technical Meetings, Change Control Board (CCB), etc.) *Standard for all projects.* | Task A -Program Management & Reporting | MS Word | Within 2 business days of meeting |
| 11 | Deliverables identified in the <Application/System Name> Project Process Agreement (PPA) | Task B System Development, Task D Operations & Maintenance | MS Word  PowerPoint | Refer to [Appendix B](#_APPENDICES).  Timeline to be provided and approved |
| 12 | Retrospective Meeting Minutes *Standard for all projects.* | Task A -Program Management & Reporting | MS Word | Within 3 business days of the end of each Sprint Cycle. |
| 13 | Future (to-be) State Roadmap *Typically for Development projects only; tailor or remove.* | Task B – System Development | MS Word | Timeline to be provided and approved |
| 14 | Version Description Document (VDD) *tailor PPA project reference artifacts; update PWS language as appropriate.* | Task B System Development, Task D Operations & Maintenance | MS Word | With every release |
| 15 | Up to five (5) non-Technical Presentations for executives, senior leaders and other stakeholders, prepared on-demand, which can cover any of the materials contained within Deliverables 2, and 11-14 *Standard for all projects, but tailor as needed based on project needs.* | Task A, Program Management & Reporting | Power Point Presentation/conference call | 5 business days after written request |
| 16 | Help Desk Guide *Remove if no Help Desk task.* | Task E – Help Desk | MS Word | Timeline to be provided and approved |

Table 6 - Programmatic Deliverables

## Continual Maintenance Deliverables

This section is standard for all Sustainment projects and can be tailored.

The contractor shall be responsible for the development and continual maintenance of the documentation identified in the approved Project Process Agreement after contract award. The contractor shall provide the updated deliverables for OIT and Product/Business Owner review and acceptance. The COR/PM shall maintain all iterations of the deliverables in the project repository (i.e. SharePoint) site with clear indication of version and date in the file name for version control and historical records. Refer to Appendix B – <Application/System Name> Project Process Agreement for listing of documentation.

Additionally, the contractor shall also be responsible for providing support in the creation and maintenance of high-level security-related documentation (include System Security Plan maintenance and other security documentation that highlights a plan to create and monitor security actions).

| **Item #** | **Document Name** | **Section of PWS** | **Initially Due** | **Update Frequency** |
| --- | --- | --- | --- | --- |
| 1 | Detailed Project Schedule/Integrated Master Schedule (IMS) utilizing MS-Project to include:   * Significant events * Documentation deliverables * UAT tasks * SDLC Decision Point tasks * Deployment tasks | * Task A -Program Management & Reporting | Schedule due within 2-weeks of award. | As changes occur |
| 2 | Risk and Issues Registers | Task A, Program Management & Reporting | With each weekly report | As changes occur |
| 3 | Section 508 Voluntary Product Accessibility Template (VPAT) and/or Certification | * Accessibility of Information and Communication Technology * Applicable Directives – Other Federal Government and USDA requirements | Prior to initial production release | Annually |
| 4 | Section 508 Compliance Testing | * Task A, Quality Assurance and Configuration Management * Task B, System Development | Scheduled at least 1 calendar month in advance of major software releases | With each major release or at a minimum annually. |
| 5 | Fully Commented Source Code, with Release Notes | * Task B, System Development * Task D, Sustainment | Within 3 business days of Release | As changes occur or within 10 business days upon receiving COR request (with delivery to FNS Enterprise TFS CCR) for each release |
| 6 | Additional CPIC, Security, and Records Management deliverables | * Task A, Project Management Support * Task B, System Development * Task D, Sustainment * Deliverables * Constraints | TBD | As needed |

Table 7 - Continual Maintenance Deliverables

# CONSTRAINTS

*This section is standard and should be included with all PWS.*

FNS desires to adopt a comprehensive and unified approach for handling the multiple systems at FNS to best fit its near-term and long-term goals. To aid this unified approach, outlined below are the technology and operating constraints for the system.

* Through each step in the task lifecycle, the program will provide the final approval on whether the approach, proposed plan and intended production aligns with the program’s needs.
* The contractor shall comply with FNS Agile Systems Development Lifecycle (SDLC) framework (see Appendices A, B & C). The contractor shall refer to, and adhere to program provided artifacts (such as guides, templates, standards, formats, documents, and reports) to develop task deliverables. The existing artifacts may include aspects from project initiation to closeout (e.g., initiation, plan, analysis and design, implementation, maintenance and operation, and closeout).
* The contractor should adhere to the program regulations from a USDA and FNS security, technology, and compliance perspective.
* The contractor may also be required to provide recommendations on additional standards or regulations that the system needs to comply with.
* The contractor shall define and gain program approval of defect resolution procedures during the development, testing (e.g., penetration testing), maintenance and operation of each task.
* Upon the completion of each task, the contractor shall conduct efficient knowledge transfer to program authorized entities that may proceed with necessary activities.
* Upon the successful completion of each task, the contractor shall transfer ownership, IP rights, and data rights to the program.
* The contractor may not publish any material or discuss this project in any public forum without the express written consent of USDA’s Food and Nutrition Service. This ban includes a prohibition against any press releases, project summaries, or case studies posted on the contractor’s website, or discussing the project in any public forums.

# BILLING

*This section is standard and should be included with all PWS.*

Payments to contracting party are divided equally by the period of performance, if the contract is a Sustainment Firm-Fixed Price contract. If the contract is Firm-Fixed Price for Development or Enhancement projects, contractor will receive proportional billing based on the number of story points that have passed User Acceptance Testing (UAT) each month of the performance period. Users must accept the work that has been completed prior to contractor receiving payment. This should be completed on a monthly basis. Invoices should be submitted electronically using the Invoice Processing Platform (IPP).

## Submission of Invoices

Invoices shall be submitted in accordance with the “Authorized Payment Schedule” for each contract/task/order.

To constitute a proper invoice, the invoice must include the following information and/or attached documentation:

1. Name and address of the business concern;
2. Invoice number and invoice date;
3. Contract number, Delivery Order number, Purchase Order number, Task Order number, or other authorization for delivery of property or services actually delivered or rendered;
4. Description, unit price, extended price, and quantity of property and services actually delivered or rendered with supporting documentation (i.e. travel receipts, etc.).
5. Shipping and payment terms;
6. Name, title, phone number, and complete mailing address of responsible official to whom payment is to be sent;
7. A certification statement saying that the funds have only been used for work for this contract;
8. Name, title, phone number, and mailing address of person to notify in the event of a defective invoice;
9. Taxpayer Identification Number (TIN) or DUNS+4; and,
10. Contractors MUST note FINAL INVOICE on the final invoice when submitted upon final delivery of all supplies/equipment or completion of the contract. USDA and the Invoice Processing Platform (IPP) – [Link to IPP.gov for Vendors](https://www.ipp.gov/vendors/index)

The IPP is a government-wide secure web-based payment information service offered free of charge to government agencies and their suppliers by the U.S. Department of Treasury’s Financial Management Service (FMS).

One-time enrollment in IPP means that you will receive a series of e-mails from Treasury services. The first email will have the IPP Logon ID and link to the IPP application. A second e-mail, sent within 24-hours, contains the password. Once you receive these emails, please login to the IPP application and complete the registration process.

Benefits of registering with IPP include the ability for your company to create invoices directly from a contract award and submit them electronically.

The IPP Customer Support Desk is available to assist users Monday through Friday (excluding bank holidays) from 8:00AM - 6:00PM ET, including answering any questions related to accessing IPP or completing the registration process. The IPP Customer Support Desk contact information is 866-973-3131 (toll-free) or [IPP Customer Support email address](mailto:IPPCustomerSupport@fms.treas.gov). If you have any questions or concerns, please contact the Controller Operations Division Help Desk at: 1-877-243-3072 or via e-mail at: [cod.help@usda.gov](mailto:cod.help@usda.gov).

# PLACE OF PERFORMANCE

*This section is standard and should be included with all PWS. Language below is for onsite; update the location and language for onsite/offsite support as necessary to meet your contract needs.*

FNS expects the contractor to be <onsite at FNS’ Office, which is located at: 1320 Braddock Place, Alexandria, VA 22314/offsite>.

FNS requires that in person meetings occur within FNS’ Office, which is located at: 1320 Braddock Place, Alexandria, VA 22314.

There is no anticipated non-local travel. In addition, FNS will not provide reimbursement costs for local travel.

# PERFORMANCE METRICS

*This section is standard and should be included with all PWS. However, tailor performance requirements as necessary for specific project needs.*

FNS will conduct performance reviews to analyze and evaluate the contractor’s performance in accordance with the following performance requirements summary. In addition to the Performance Metrics identified below, the contractor is encouraged (optionally) as part of their proposal submission to identify additional performance requirements (task or deliverable, performance standard, acceptable quality level, surveillance method, and performance rating) and describe how such additional measures will affect performance. Invoices will be held by COR, with approval from CO, for failure to submit deliverables that meet all requirements and delivered within the time frames established within the PWS (unless government at fault for delay).

| **Required Activities** | **Performance Standards** | **Acceptable Quality Levels (AQL)** | **Methods of Surveillance** | **Contractor Required**  **Action for Quality** |
| --- | --- | --- | --- | --- |
| Timeliness of Onboarding Process | Contractor responds to any onboarding processing requests within 48 hours, copying COR, as outlined in the Onboarding Process. | 100% | Review of emails sent to COR | Responding within 48 hours; Ccing COR on any email received to verify response. |
| Use of GFE, user accounts and FNS email | In accordance with USDA policies regarding IT usage; all personnel performing functions within IT (non-privileged and privileged rights) are required to use government furnished equipment, assigned user accounts and FNS email. | 100% | 100% Inspection | Use only GFE, not personal equipment, FNS approved accounts, and FNS email for official business. |
| Level of Effort (LOE) Estimates/Story Points | Baseline – 3 days after completion of Sprint Zero;  Thereafter maintain 1.5 – 2.0 Sprints worth of user stories estimated based on Product/Business Owner prioritization. | 100% | * Review documentation via independent verification. * Review Sprint documentation. | * Delivered on time. * Time and cost estimates are off by no more than 10%. |
| Timeliness of Deliverables/Delivery | Contractor submits all required deliverables to include project schedule, management reports, sprint artifacts, and releases on time with no significant defects. | 90%  95% | File reviews, periodic inspections, and/or random observations. | * Deliverables are submitted on time, unless approved by the COR * Project Schedules are submitted on time 95% of the time. |
| Software Quality - UAT | * Defects by severity/day; * Number of resolved/ unresolved defects | 95% | Review of Test Plan Results | Provide defects tracking metric information in UAT Test Plan Results |
| Software Quality - Production | Defects by severity/type | 95% | Review of User Stories | Provide defect tracking metric information in Weekly Status Reports/Monthly Status Report identifying defect severity. |
| Documentation Deliverable Quality | Documentation is delivered that is Accessible, and free of Major or Catastrophic defects categorized as: clarity, graphics, detail, editorial, flow, requirements, standards, or other. | 95% | Accessibility Verification and COR Review of Documentation | Deliverables are submitted defect free and proof of appropriate Accessibility Checker results provided to COR at time of delivery. |
| Configuration Management (CM) | Approved CM processes and procedures are followed | 100% | Review of the CM system used | Appropriately name and maintain all CM deliverables; follow CM procedures accordingly. |
| Team Foundation Server Source Code Upload | Source code is uploaded into the FNS Enterprise TFS CCR within 3 business days after deployment to Production | 100% | Review of TFS logs | Deliverables are submitted on time, unless approved by the COR |
| System Changes | No systems changes are done without coordination with FNS Product Owner and at the COR’s approval. | 100% | Review of Status Report | Changes are coordinated with FNS and approved by the COR through CCB process. |
| Application Availability | Applications are available to perform required work within the scope of vendor support. | 99.60% | 100% Inspection | Application availability, not related to network or hosting facility. |
| FedRAMP Compliance | Contractor must adhere to FedRAMP requirements for PII Cloud Service and continuous monitoring guidelines. See Appendix C. | 100% | File reviews, periodic inspections and/or random observations, customer complaints. | Documented process change including greater oversight to meet AQL. |
| Security Compliance | Security Compliance metric measured per release. Data collection from data gathered by the Problem Management and Configuration Management Processes. Includes application scans and vulnerability error remediation based on FNS identifies standards, such as BOD 18-02, 19-01, 19-02, DR3830.006, and DR3565.003. | 100% of Critical and High vulnerabilities | 100% Inspection | Vulnerabilities are remediated according to BOD 19-02 and deviations are documented following DR 3565-003 Plan of Action and Milestones Policy. |
| Security Documentation | Contractor provides security documentation update information as requested. | 95% | Observation, file review. | Documented process change including greater oversight to meet AQL. |
| Disaster Recovery (DR) Training & Exercise Support | Contractor provides appropriate staff and documentation to support semi-annual or other schedule DR exercise and training support | 100% | Observation, file review. | Initial Release and annually thereafter. |
| Help Desk – Ticket Age (Open Tickets) | This is a measure of the age of tickets not in the Deleted, Solved, or Closed statuses. | 100% | Review of Help Desk Reports | Help Desk Report showing max age between the ticket created date to the present by Ticket ID where ticket status is not Solved, Deleted, or Closed; provided on a monthly basis |
| Help Desk - Time to First Response | This is a measure of how long it takes, on average, for a customer to receive an initial reply from a support agent. | 95% based on criteria in Section <X.X> of PWS | Review of Help Desk Reports | Help Desk Report showing average time to first respond weekly and monthly. |
| Help Desk - Average Customer Wait Time | Measures the entire customer experience from ticket creation to resolution. | 95% based on criteria in Section <X.X> of PWS | Review of Help Desk Reports | Help Desk Report showing average customer wait time from ticket creation to resolution. |
| DBA support services | Contractor coordinates with FNS for all activities that require extensive use of the database or takes the database out of production | 100% | File reviews, periodic inspections and/or random observations, customer complaint. | TBD |
| Database error correction and issue responsiveness | Contractor addresses all “Critical”\* trouble reports involving any of the database servers within 2 business hours and/or “Serious”\*\* trouble reports involving any of the database servers within 4 business hours and worked on as a top priority until resolved.  Contractor addresses other trouble reports of the database within 8 business hours and worked on as directed. | 100% | File reviews, customer complaint. | Documented process change including greater oversight to meet AQL. |
| Database maintenance and reporting | Contractor provides electronic format ad-hoc reports from data within the databases as directed by senior FNS staff | 95% | File reviews, periodic inspections and/or random observations, customer complaints. | Documented process change including greater oversight to meet AQL. |

Table 8 - Performance Metrics

**Note:** For database error correction and issue responsiveness:

\* “Critical trouble reports” = problems with the system that prevent all users from using the system.

\*\* “Serious trouble reports” = problems with the system that prevent some users from using the system or portion of the system.

# APPENDICES

| **Appendix** | **Title** | **Reference** |
| --- | --- | --- |
| Appendix A | FNS Agile SDLC Guide |  |
| Appendix B | Project Process Agreement (PPA) | <Insert Object for approved project PPA with applicable SDLC templates> |
| Appendix C | FedRAMP for Cloud Service Providers (if required) | [Link to FedRAMP for Cloud Service Providers](http://www.fedramp.gov/cloud-service-providers/) |
| Appendix D | NIST Special Publication 800-122 | [Link to NIST Special Publication 800-122 download](https://csrc.nist.gov/publications/detail/sp/800-122/final) |
| Appendix E | NIST Special Publication 800-171 | [Link to NIST Special Publication 800-171, Revision 1 download](https://csrc.nist.gov/publications/detail/sp/800-171/rev-1/final) |
| Appendix F | Department of Homeland Security - Binding Operational Directives | [Link to DHS Binding Operational Directives webpage](https://cyber.dhs.gov/directives/) |
| Appendix G | Office of Management and Budget M-15-13 | [Link to OMB M-15-13](https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2015/m-15-13.pdf) |
| Appendix H | NIST Special Publication 800-53 Revision 4 | [Link to NIST Special Publication 800-53 database](https://nvd.nist.gov/800-53) |
| Appendix I | FNS Approved Software List | <Insert Object for latest FNS Approved Software List with date> |

Table 9 – Appendices

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 is used to meet international standards after the release of the Section 508 Refresh. [↑](#footnote-ref-2)