United States Department of Agriculture (USDA)
Research, Education, and Economics (REE)
Office of the Chief Information Officer (OCIO)
Information Technology Services Division (ITSD)

Performance Work Statement (PWS)

Information Technology Security Assessment and Authorization (A&A)

Risk Management Framework (RMF) Step 1 -3 for

ERS Coleridge (formerly NYU ADRF)

TABLE OF CONTENTS

1. PURPOSE

The USDA REE Mission Area has a need to obtain contract support for Assessment and Authorization (A&A) of ERS systems and applications using the NIST Risk Management Framework (RMF) Step 1-3b, Information Technology Security Assessment and Authorization which includes developing specific security plans and documentation that meets USDA requirements for documenting security controls and for certifying and accrediting the system in accordance with applicable National Institute of Technology (NIST) Special Publication (SP) 800-53, Rev 4 (or latest Version) Security Control requirements and documenting the results of the A&A into the USDA Cyber Security Assessment Management (CSAM) tool.

The purpose of this requirement is to obtain technical support and to develop specific documentation that meets or exceeds FISMA compliance and USDA's requirements for Steps 1 -3b of the RMF. These requirements consist of all tasks necessary for RMF Steps 1-3b.

2. BACKGROUND

Federal law and Office of Management and Budget (OMB) guidance require that agencies establish oversight mechanisms, systematically evaluate, and ensure the continuing security, interoperability, and availability of systems and their data. Specifically, the guidance requires a process, called "security accreditation," for each system.

Security accreditation is the official management decision to authorize operation of an information system. Security accreditation provides a form of quality control and challenges managers and technical staff at all levels to implement the most effective security controls and techniques, given technical constraints, operational constraints, cost and schedule constraints, and mission requirements. The accreditation decision is based on the implementation of a security plan, risk assessment, and other supporting documents. Systems must be accredited before beginning operation or after any significant change that could affect the protection of the system. In addition to continuous monitoring and continuous assessment requirements, USDA additionally requires that systems must be re-accredited at least every three (3) years, the end result being reflected in an official Authority to Operate (ATO) memorandum accepted by USDA – Office of Information Security (OIS), Compliance, and Policy Branch (CPB).

In addition to security plans and other supporting documents, security evaluation plays an important role in the security accreditation process. This evaluation determines the effectiveness of these security controls in a particular environment of operation and the vulnerabilities in the information system after the implementation of such controls. The results of the security certification are used to reassess the risks and update the security plan for the information system—thus, providing the factual basis for the authorizing official to render the security accreditation decision.

The United States Department of Agriculture (USDA) has developed its own Risk Management Framework (RMF) Process Guide that is intended to provide a comprehensive and uniform approach to the RMF process. Individuals responsible for, or involved in the USDA RMF process, will use this guide as a resource to assist them in certifying and accrediting USDA systems. This guide and the CPB mandates the use of the Cyber Security Assessment and Management (CSAM) tool, which incorporates information and standards directly from National Institute of Technology (NIST) Special Publication (SP) 800-53 Revision 4, (or latest

Version) Recommended Security Controls for Federal Information Systems and NIST SP 800-53A Revision 1, Guide for Assessing the Security Controls in Federal Information Systems.

3. SCOPE OF WORK

USDA REE is seeking RMF Step 1 -3b (A&A) support for **one (1) ERS IT system**.

1. ERS Coleridge (formerly NYU ADRF) (ERSNYU)
    a. FIPS 199 Categorization: Moderate
    b. System

Specific requirements are described in the USDA Seven Step RMF Process Overview. The vendor shall provide support to the USDA ERS comprising of the following area:

- **RMF Step 1 – 3b –** Security Plans and Documentation Reviews

RMF Contractors that perform RMF Step 4, (Formerly A&A Phase 2) on any system must not perform RMF Step 1, (Formerly A&A Phase 1) on that same system, and vice versa.

The Contractor must certify that they have not performed RMF Step 1-3b and 4 on a system within the same accreditation cycle. **Attachment 2, Conflict of Security Interest and Disclosure** must be completed and submitted with the Contractor's proposal to the requesting Contracting Officer via email at: Jessica.Edwards2@usda.gov

Performing both RMF Step 1-3b and RMF Step 4 on the same system within the same accreditation cycle violates USDA (OIG, OIS-CPB) accepted best practices to ensuring independence and separation of duties. Violations may result in contract termination. The Government may take additional actions, as well.

The same Contractor cannot perform both RMF Step 1-3b and RMF Step 4 regardless of the FIPS199 (Low, Moderate or High).

These requirements consist of the tasks for RMF Step 4 and 6 as noted in the aforementioned USDA RMF Process Guide and this PWS.

USDA has its own RMF Process Guide, required USDA templates and concurrency review checklists to provide a comprehensive and uniform approach to the RMF process. The guide is a resource to assist agencies in certifying and accrediting USDA systems. The USDA checklist provides a brief overview of the critical steps that must be completed to complete this part of the NIST 800-37 revision 1 process for Steps 4 and 6.

The Compliance, and Policy Branch (CPB) will provide updated templates and checklists to assure that the contractor has the information to ensure that the documents developed conform to USDA/OIS/CPB guidelines/regulations. These templates should not be altered or substituted, and any deviations should be approved by OIS CPB.

4. SF 1449 CONTINUATION

a. Administered By:

ERS Contracting Officer: **Jessica Edwards**

The USDA Technical Project Manager (TPM) is: TBD

ERS Coleridge (formerly NYU ADRF):

b. Invoice Submission:

Invoices for payments must be submitted electronically through the Invoice Processing Platform (IPP) via www.ipp.gov. Partial payments will NOT be made for incorrect invoices. Invoices cannot be certified without the corresponding progress and labor report.

NOTE: Approximately 25% of the Contractor's final invoice payment will be held until the agency receives CPB acceptance Phase 1 or 2 (Concurrency Review Acceptance/Concurrence/Approval Memorandum).

In addition, the Contractor's invoice must be completely detailed to include, but not be limited to: Order number; period of service, full description of services provided; labor category (if applicable); contract line item billed against; number of hours billed against the specific line item; unit price; extended price; invoice total; Contractor name, address, telephone and contact person; invoice number and date; and GSA Federal Supply Schedule Contract number.

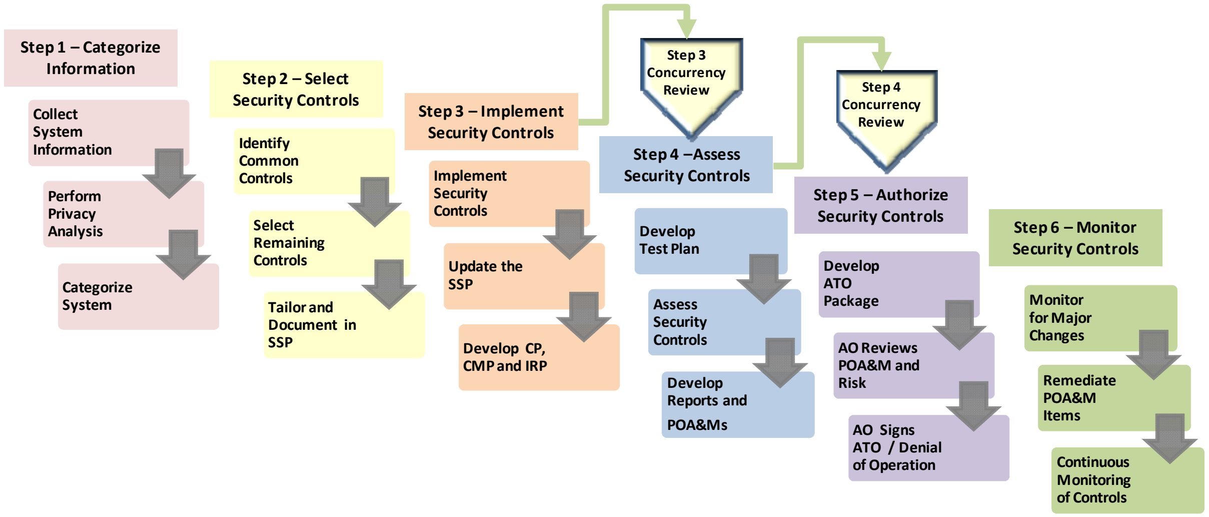
c. Contract Type:

This is a **Firm Fixed Price** task for performance based commercial services. **Note:** "Travel must be included as a separate line item on the Contractor's proposal and on the purchase requisition and not rolled up into either of these Fixed Price rates.

5. USDA Six Step RMF Process Overview

These instructions provide the accepted methodology for conducting a NIST and USDA compliant A&A of IT systems and performing the corresponding CSAM data entry of all results and required documentation. All USDA agencies must follow the seven-step approach to achieve an ATO and to effectively manage risk for their systems. The Department uses CSAM as its automated FISMA management tool and the system of record to capture system information throughout the A&A process. At USDA, all system information, documentation, and assessment results are required to be recorded in CSAM.
Below is a diagram of the six step RMF process.

USDA RMF Process


Step 1 – Categorize Information
Collect System Information
Perform Privacy Analysis
Categorize System
Step 2 – Select Security Controls
Identify Common Controls
Select Remaining Controls
Tailor and Document in SSP
Step 3 – Implement Security Controls
Implement Security Controls
Update the SSP
Develop CP, CMP and IRP
Step 3 Concurrency Review
Step 4 –Assess Security Controls
Develop Test Plan
Assess Security Controls
Develop Reports and POA&Ms
Step 4 Concurrency Review
Step 5 – Authorize Security Controls
Develop ATO Package
AO Reviews POA&M and Risk
AO Signs ATO / Denial of Operation
Step 6 – Monitor Security Controls
Monitor for Major Changes
Remediate POA&M Items
Continuous Monitoring of Controls

Risk Management Framework

USDA has implemented a continuous assessment/continuous monitoring methodology for achieving a system/program ATO. New systems, systems undergoing a major change (for definition of major change see Section 2.9) or systems that have never been through the complete RMF Process must complete the RMF steps as described below starting with Section 2.1. All other systems shall follow the ongoing assessment and authorization methodology as presented in Section 2.8.

5.1 RMF Step 1: Categorize the Program/System

Step 1 of the RMF focuses on the collection of general system information, completing the Privacy Threshold Assessment (PTA), Privacy Impact Assessment (PIA) and completion of the FIPS PUB 199 system categorizations. This collected information includes the mission, environment, boundary definition, architecture, and information the system transmits or processes. The system owner is responsible for completing the categorization and may require the participation of the information system security officer or others as needed.

Requirements for All Systems/Programs	Potential Additional Requirements

• Collect general system information • Create CSAM entry and enter information • Create PTA and upload to CSAM • Perform security categorization • Enter remaining information in CSAM System Identification (Purpose, attributes, funding, etc.) and Narratives (System description and Technical description)	• Perform PIA and upload to CSAM • Perform E-Authentication Risk Assessment and upload to CSAM (under Appendix G5: E-Auth Risk Assessment OMB M04-04)

Table 1-1: RMF Step 1 Requirements Summary

5.2 Collect System Information

Before beginning the categorization process, it is helpful to have the following information readily available: system and/or network diagrams; a description of the system's mission/purpose; business impact assessments; privacy impact threshold/privacy impact assessments; and contingency, disaster recovery, incident response, or configuration management plans. Systems in development will not have all of this documentation, but at a minimum will need to obtain information from the system's detailed design documentation.

While gathering information, it is best to start by populating the basic system information into CSAM. Any of this information can be updated as the system moves through the process. The CSAM headings of "System Information” (Identification, Locations, Relationships, Narratives and Points of Contact), are areas that need to be filled out and completed before moving on to security categorization activities.

5.3 Perform PTA, then PIA if needed

With the information from section 2.1.1 gathered, perform a PTA based on the template in Appendix B. If indicated by the PTA, perform a PIA based on the template included in Appendix B. If privacy information and/or special handling are indicated by the PIA, then consideration of this is required during the next step - security categorization. Note: There shall be one PTA for each SSP and at most one PIA for each SSP.

5.4 Security Categorization

The primary goal of this step is to utilize NIST SP 800-60 Rev.1, *Guide for Mapping Types of Information and Information Systems to Security Categories (Volume 1 and Volume 2)* in accordance with FIPS PUB 199 to categorize the information system. The System Owner categorizes the information within the information system to determine the impact that a compromise of confidentiality, loss of integrity, and/or the lack of availability would have on the mission of the agency. This impact determination (low, moderate, or high) establishes the security control baseline applicable to the system. The system categorization is entered into CSAM from the “System Information” – “Information Types" section.

To perform a security categorization of any system requires knowledge of what information is contained within the system. It is important to determine the value of this information from the standpoint of confidentiality, integrity, and availability (CIA). This information is then utilized to determine the generic data categories from NIST SP 800-60 Revision 1 *Guide for Mapping Types of Information and Information Systems to Security Categories: Appendices* with their default values of high, moderate, or low for the CIA areas. The data categories equate to information types in CSAM. The default CIA values for each information type are also pre-populated in CSAM. Based on the value of the information in the system, these default values can be modified to be either more or less critical, as illustrated in the example below.

Once all the information types have been defined and values have been assigned, the overall categorization of the system is the highest value identified for any of the categories. This is referred to as the "high water mark". For any assigned values (low, moderate, high) that differ from the NIST recommended values, an explanation or justification must be entered that clearly explains the reason for the change from the NIST recommendation.

Systems that are made up of other systems/applications must include the information types for all the systems/applications involved. General support systems (GSS)/Major applications (MA) are categorized to the highest level of any of the applications/systems that reside on the GSS/MA. Note that the presence of Privacy Information requires the confidentiality of the system to be at least a Moderate.

Information Category	**Confidentiality Rating (C)** (*H,M,L*)	**Integrity Rating (I)** (*H,M,L*)	**Availability Rating (A)** (*H,M,L*)	**Privacy**	**Financial**	**Medical**	**High Water Mark**
Budget and Finance	M	M	L		X		
Immunization Management	M[1]	M	L	X		X	
**Highest Impact*	**M**	**M**	**L**	**X**	**X**	**X**	**M**

Footnotes:

[1] Some information associated with immunization management involves confidential patient information subject to the Privacy Act and to HIPAA.

5.5 RMF Step1 Completion Summary

- Collect information about the system, including specifics about what information the system will process, transmit, or store. Create a system/program security plan (SSP or just SP) entry in CSAM for the system and enter the general information.
- Perform a PTA based on the actual information contained in the system. If the PTA requires a PIA to be completed, then perform a PIA. Upload the PTA/PIA to CSAM.
- Perform the E-Authentication Risk Assessment and post it to CSAM Appendix G-5, if appropriate. Please see Section 3.6.
- Complete the categorization of the system in the CSAM Information Types tab by selecting the NIST SP 800-60 Revision 1 data categories that correspond to the actual information the system processes. If any risk levels (high, moderate or low) are changed for an information type, then document the reason.
- Completely describe the system by entering remaining information into CSAM to include the system's locations, interfaces, narratives, and points of contact.

- Register the system with other corresponding Departmental systems such as the Agriculture Maximum (AgMAX) and/or Enterprise Architecture Repository (EAR). Ensure the Office of Management and Budget (OMB) 300/53 identifier and name in CSAM matches those in the other systems.

5.6 RMF Step 2: Select Security Controls

Just as FIPS PUB 199 and NIST SP 800-60, Rev. 1 are mandatory processes for the categorization of information systems, FIPS PUB 200 and NIST SP 800-53, Rev. 4 are mandatory processes for the selection of the corresponding security control baselines. Once the FIPS PUB 199 security categorizations of the information system is documented in CSAM, select the high water mark for the categorization and set that categorization in CSAM for the system. Once this is accomplished, the corresponding set of controls (high, moderate or low) will automatically be selected for the information system within CSAM. This security control baseline must then be tailored within CSAM to include the selection of inherited controls and the documentation of the implementation of each control.

Requirements for All Systems/Programs	Potential Additional Requirements
• Identification of all common/inherited controls • Compliance descriptions identified for every control including tailoring • Create any needed compensating controls • Develop Contingency Plan (CP), CP test training and testing documents	• 508 Compliance • System of Record Notice (SORN) • Configuration Management Plan (CMP) • Incident Response Plan (IRP) • Disaster Recovery Plan (DRP) • Interconnection Security Agreement (ISA) (Optionally, this could be in the form of a Memorandum of Understanding (MOU) or Service Level Agreement (SLA))

Table 2-2: RMF Step 2 Requirements Summary

5.7 Identify Common/Hybrid Controls

The selection of common controls is one of the first tasks that must be accomplished. A common control is a control that can be applied *in its entirety* to one or more organizational information systems. The control must be designated, assessed, and approved in writing as a common security control. There are a few points to remember when selecting common controls:

- Controls need to be inherited from the system that provides that service or capability. In other words, a program does not actually perform virus scanning, so the virus scanning controls cannot be inherited from a program. However, the virus scanning control could be inherited from the network or system the application resides on.
- Every common control (including the common portion of a hybrid control) must identify the exact program/system that the control is common to. The program/system should have: (1) a control implementation that satisfactorily documents the control in terms broad enough to include the systems that should inherit the control; and (2) tested the control as part of an A&A.
- Hybrid controls require a further explanation as to what is being inherited along with the name of the program/system from which it is being inherited.

- The following control restrictions exist:
    - The following NIST SP 800-53, Revision 4 controls are system-specific controls and cannot be common, hybrid, or not applicable: AU-2, AU-2(3), CA-2, CA-2(1), CA-2 (2) (for high systems), CA-3, CA-3 (5), CA-5, CA- 6, CM-2, CM-2(1), CM-2(3), CM-4, PL-2, PL-2 (3), RA-2, RA-3, SA-5.
    - For systems that contain PII – these controls are not common, hybrid, or not applicable: AP-2, AR-7, and DM-2.
    - For systems that contain PII – these controls are hybrid with the department, they cannot be common or not applicable: AP-1, TR-1.
    - For systems that do not contain PII: All the privacy controls including all their enhancements must be made N/A with the reason that the system does not contain privacy information.
    - The CP-2 and CP-4 controls can be common controls if the CP for the system in question is: (1) a CP that covers multiple systems or a GSS; and (2) the control was previously tested during the assessment of another system covered by the CP. If the system has its own CP, these are system specific controls.
    - The Program Management (PM) family of controls can be inherited from the USDA Departmental Common Controls. The agencies should make any of these controls hybrid if they have additional policy or procedures that are pertinent.
    - "Dash-1" controls -- the first control of each control family – address Departmental policies and Agency procedures. The Dash-1 controls should be hybrid with the Department-level implementations offered by USDA Departmental Common Controls. The Department is responsible for the creation of the policies pertaining to the controls. The agencies are responsible for all control procedures, unless otherwise specified by the Department. Agencies may create policies that exceed the baseline guidance published by the Department but must follow Departmental policy. CA-1 should be inherited from the Departmental Common Controls in its entirety, because the Department issues the policy and the procedures.

Common controls are selected and assigned in CSAM. As agencies update the systems with the proper inheritance, issues may arise where a control implementation that is required to be inherited from a program/system cannot be. These controls should be made "Not Applicable" in CSAM. When making the control not applicable, enter the complete explanation of the inheritance (what is inherited and from what system is it inherited from) as the justification.

5.8 Tailoring Remaining Controls and Document in CSAM

Once the selection of common controls is accomplished, evaluate the remaining controls to determine which will be hybrid and which will be system specific. This is also a good opportunity to look at controls that are not applicable. Not-applicable controls must have a valid reason/justification explaining why they are not applicable. An example is the Voice over Internet Protocol (VoIP) control. This could be designated as not applicable because the system does not contain or use VoIP.

Once the decisions have been made as to what controls the system must implement, a strategy for continuous monitoring of the controls must be developed and any required changes to the control tailoring must be made. For a new system that has never been through the process, the Authorizing Official (AO) will approve the security plan at this point. This approval designates those controls that must be implemented by the system.

Most systems at USDA are operational with controls in place, therefore steps 1 through 3 have already been accomplished. For these systems, the SSP and associated documentation must be reviewed/updated annually by the system owner. This is covered in Section 2.8.

5.9 Develop a Strategy for Monitoring the Controls

The Department establishes the criteria for selecting security controls to be monitored (post deployment) and determines the frequency of the monitoring for Key and annual sets of controls. The Department has established the monitoring criteria and frequency for all controls in the Department. (See Appendix E for the list of controls and the year of their assessment). The agency can monitor controls more frequently but cannot monitor them less frequently.

All control assessments for moderate/high categorized systems must be accomplished by an independent assessor. The owner(s) of any controls inherited by the system is responsible for the annual assessment of those controls and the system will inherit the result.

5.10 RMF Step 2 Completion Summary

- In the “Assessments – Control Management” section of CSAM, ensure the NIST Version is set to NIST SP 800-53 Rev4 (or latest Version) and the “Controls on prior Control Sets” field value is zero (0). (Please review the OIS/CPB Resources SharePoint site for information on migrating the control set to Rev. 4.)
- Inherit common controls from those offered in the inheritance selection area for which the system in question has permission.
- Enter compliance descriptions for all controls not inherited.

5.11 RMF Step 3a: Implement Security Controls

RMF Step 3 focuses on the implementation of security controls during system development and/or after the system has been developed. Implementation of the security controls is the responsibility of the System Owner and/or the common controls provider where controls are inherited. Once the controls are implemented, the SSP compliance descriptions, CP, CMP and IRP should be finalized to capture the true “as-built” implementation. A CMP, IRP, and CP may need to be developed for the system unless these are covered under another plan elsewhere in the hosted environment.

Requirements for All Systems	Potential Additional Requirements
• Finalize SSP compliance descriptions • Finalize CP	• 508 Compliance • Finalize CMP, IRP and DRP (If required)

Table 3-3: RMF Step 3 Requirements Summary

5.12 RMF Step 3.1: Implement Security Controls

The primary task of this step is to document every applicable security control in the security plan. Be clear and address all aspects of the control. Use a 12-point Times New Roman Font. If the control has an A, B, and C, then the implementation should have an A, B, and C, followed by the implementation of each aspect of the control. This makes it easier for the security controls assessor and the concurrence review team to ensure that each aspect of a control is properly addressed and implemented. It is best to consider the NIST SP 800-

53 control to be a statement of policy and the implementation a write-up of exactly how the program/system implements that statement of policy. Therefore, it is unnecessary to quote policy in the implementation.

5.13 RMF Step 3.2: Update the SSP

Once all of the security controls are complete with implementations entered, generate the security plan in CSAM. Once generated, review the plan, checking to be sure that control implementations have indeed been entered into CSAM. Conduct a search of the plan for any blank fields. There should be no blank fields within the SSP; every field should have something entered. If not, go back to the control implementation and determine why the field is blank.

5.14 RMF Step 3.3: Finalize the CP, CMP and IRP

It is at this step that all the documents need to be updated to reflect the current state/implementation of the system. If the system is covered by an organizational CMP and IRP, then ensure these inherited documents contain specific references to the system. The CP should be finalized along with the CP test plan, training and CP test results. Specified inherited documentation should be specifically referenced as to their location, while system specific documentation should be loaded in CSAM to their Appendix locations following the guidance of Section 3.1.

Below is a checklist for RMF Step 3 major items that must be completed before submission for concurrence review:

- Finalize and post the CP, CP training, and CP test documentation to CSAM Status Page (post to the CSAM System & Status Archive Page, then to CSAM Appendix L).
- Finalize and post the IRP to the CSAM Appendix O. Either inherit it from the Department/agency or develop a system specific one.
- Finalize and post the CMP to the CSAM Appendix Q.
- Finalize and post an ISA/MOU/MOA to the “System Information” – “Relationships” tab for each system connection.
- Send an email to the Cyber Communication mailbox (cscc@ocio.usda.gov) requesting an RMF Step 3 Concurrence Review.

5.15 RMF Step 3b: Concurrence Review

When the SSP is complete, it needs to be submitted for RMF Step 3 concurrence review. The user submits an email to the concurrence review team at cscc@ocio.usda.gov stating the package is ready for review in CSAM.

This concurrence review is primarily for the security plan and the categorization; however, the supporting documents (CP, CMP, ISA, PTA, and/or PIA) that are present at the time of the review will also be considered. If the concurrence review team finds any issues with the documentation, they will notate the issues in the concurrence review checklists and return the checklists to the agency. The key items for the RMF Step 3 review are the system categorization and the security plan. Since issues with the remaining documents do not have a significant effect on testing, they can be addressed simultaneously with the performance of RMF Step 4 testing.

The result of the concurrence review is either passage of the system to RMF Step 4 (Assess Security Controls), or the documentation is returned for further refinement with a checklist of items to remediate. Agencies cannot proceed to RMF Step 4 until notified via concur memo that the system has successfully completed the RMF Step 3b concurrence review. If the documentation is returned with a remediation checklist noting issues identified with the security plan, system categorization or other documents to be addressed, the system must be re-submitted to the concurrence review manager for verification that the issues have been adequately addressed.

Upon satisfactory completion of concurrence review, the concurrence review manager will ensure that the RMF Step 3 concur memo is issued. Once the RMF Step 3 concur memo is issued, the SSP shall not be modified without first discussing the changes with the OIS liaison and the concurrence review team. The SSP should not be unilaterally modified by the System Owner until after the program/system is authorized to operate.

Below is a checklist for RMF Step 3 concurrence review:

- Security plan/system notification submitted via email to the Cyber Communication mailbox (cscc@ocio.usda.gov) for RMF Step 3 concurrence review.
- Concurrence review comments for RMF Step 3 received (completed checklists).
- Security plan/system updated based on concurrence review comments.
- Security plan/system re-submitted via email to the Cyber Communication mailbox for RMF Step 3 concurrence re-review.
- Program/system RMF Step 3 review completed (agency receives concur memo stating RMF Step 3 concurrence review has passed).
- Program/system Concur Memorandum from OIS CPB posted to the CSAM Status & Archive Page to Security Authorization section and then post to CSAM Appendix H.

Concurrence review team will generate the Security Plan and post it to CSAM Appendix F(*x)* with the title "FY19 A&A Security Plan". ("x" means the next consecutive numbered "F" appendix -- this is the A&A archive copy).

5.22 Mandatory Concurrency Review Training/Briefing

All contractor employees performing tasks within this PWS are required to undergo USDA, OCIO, and CPB's Concurrency Review Training. USDA's RMF includes a mandatory concurrency review process to ensure that the tasks performed with regard to security assessments outlined in this PWS are in accordance with NIST and compliant with FISMA. Proof of compliance with this requirement must be established by providing the COR and TMP with a Certificate of Completion issued to the Contractor by USDA, OCIO, and CPB prior to beginning tasks.

6. CYBER SECURITY ASSESSMENT MANAGEMENT (CSAM) OVERVIEW FOR A&A

The Cyber Security Assessment and Management (CSAM) tool is a comprehensive Federal Information Security Management Act (FISMA) compliance monitoring tool developed by the Department of Justice (DOJ). CSAM facilitates the ability to identify common threats and vulnerabilities; supports a security control baseline to achieve FISMA compliance; and provides comprehensive information technology (IT) weakness tracking for the following:

a. Complete Plan of Action and Milestones (POA&M) tracking and management;
b. Integration of A-123 Appendix A and FISMA;
c. Accurate Security Categorizations and Identification of financial systems;
d. Identification of Core and Common Controls;
e. Application of National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Rev. 4 (or latest Version) Security Controls to meet both FISMA and A-123 Appendix A;
f. Continuous monitoring of Security Controls;

g. Collection and Analysis of Control Compliance information; and
h. A Repeatable Process that continually Assesses Controls Effectiveness.

The CSAM tool improves agency security identification and management processes, shares lessons learned and facilitates best practices. CSAM assists agencies with their A&A requirements, provides quality POA&Ms and improves system security plans for a robust IT security process.

The following is a summary of major areas of interest in CSAM, which the contractor shall review, develop, modify/update, or maintain, in accordance with USDA A&A/RMF Process and Guide Overview and as required by USDA CPB.

a. Risk Management

CSAM aligns threats and vulnerabilities to a system's operational boundary. The National Institute for Standards and Technology special publications is used as the foundation for functionality. NIST security controls incorporated into CSAM allows implementers and testers to close the gap so that requirements are more easily satisfied.

b. Enterprise Program Management

Agency security programs can be implemented in CSAM to allow for common security controls to be inherited by each agency system. In most situations, most security control requirements can be inherited from a general support system or site. Potential threats and the impact of a threat can be easily identified and mitigated through using CSAM.

c. System Security Plans

CSAM supports the creation and updating of a system's security plan required. Each SSP has the ability to be continuously monitored and updated throughout the system life cycle. Not only does CSAM provide for Security assessment and accreditation requirements to be kept current; it also allows for findings to be identified early within the system upgrades/enhancements. The following are some of the SSP components CSAM contains:

- Certification Results
- Change Control Board Charter
- Contingency and Disaster Recovery Planning
- Configuration Management
- Incident Response Planning
- Memorandums of Understanding
- Risk Assessment Results including supporting documentation
- Plan of Action and Milestones agency approval process
- Rules of Behavior
- Plan of Actions and Milestones including supporting documentation
- Privacy Threshold Analysis
- Privacy Impact Analysis
- Security Awareness and Training Plans and Procedures
- Security Test and Evaluation Plans and Procedures
- System Interface information and artifacts
- Systems of Records Notice

This information relative to CSAM is provided for informational purposes only.

d. Privacy Impact Assessment (PIA)

Complete the PIA, which ensures the agency thoroughly examined the privacy implications of system data collection. Specifics are outlined in the A&A guide. In addition, if required, publish a Systems of Records Notice (not applicable).

e. Contingency Plans

USDA agencies and officers are required to develop and implement an executable Disaster Recovery and Business Resumption plans for each critical system or application to ensure core business functions can be restored to full operation with minimum downtime in the event of a disruption or disaster. More specific plan requirements are provided in OCIO contingency planning guidance. Plans developed for A&A must conform to USDA guidance and be located in CSAM.

f. Identify Security Controls and Construct a Compliance Matrix

The controls should be compiled from USDA Cyber Security Manual 3500; OMB A-130; NIST 800-53, Rev 4; FISMA; and Industry Best Practices. The matrix should list each security control, the reference from which security control was derived, and whether or not the control has been implemented. (See NIST Web Page for document 800-53, Rev 4)

g. Configuration Management Plan

USDA agencies are required to develop configuration management plans to provide a disciplined and documented establishment of configuration change requests and control changes to them. These change requests are adequately assessed and responded and tracking documentation throughout the development process by establishing a configuration control board.

h. Interconnection Security Agreement (ISA) (High, Medium, Low Systems)

If system is being connected to other IT systems, the business owner must discuss the requirements for connectivity with other system's business owner and work to identify the security requirements for this connection. An ISA must be completed for each system that will be connected to the new system. See USDA A&A guide for further guidance.

7. KICK-OFF MEETING, Project Schedule, Weekly Status Reports, Meetings, Travel

a. Kick-off Meeting and Project Schedule

A Kick-off Meeting will be scheduled within five business days after award and may be conducted remotely at the discretion of the TPMs. The Contractor shall provide a draft schedule of their Project Plan to meet the customers' requirements as identified in this statement of work with their proposal. The Contractor at the Kick-off meeting should provide a Project Plan (with Strategic/Tactical Plan outline or table of contents as well as milestones). The Contractor shall identify the specific priorities and establish schedule details and identify key personnel involved. Any changes or adjustments to this schedule will be coordinated with the USDA TPMs.

The Contractor's presentation and discussions shall contain the following minimum requirements:

A. Project Plan. A detailed Project Plan including recommended timelines, deliverables, and milestones necessary to accomplish the scope of work and technical requirements of this PWS. The Final Project Plan shall be mutually agreed upon by both the Contractor and the USDA

B. Required Security Authorization activities

C. Define roles and responsibilities of project team members

D. Concurrency Review Training status

E. Quality control of deliverables

b. Weekly Status Reports

The Contractor must provide weekly status reports that shall be emailed to the USDA TPMs by 12 noon, (ET), Tuesday of each week. The weekly status report shall include, as appropriate: significant accomplishments, problems and difficulties encountered, and issues needing resolution by the TPMs. Electronic format using MS Word for reports and Excel for spreadsheets is the preferred method for submission. The USDA TPMs may require that a report be submitted sooner than Tuesday of each week.

c. Weekly Project Status Meetings

The Contractor shall conduct weekly project status meetings to include oral briefings on the Security Authorization status and issues. Meetings will be held virtually on Tuesday of each week. Weekly meeting may be negotiated at the discretion of the CO and/or TPMs. The Contractor shall organize and convene a formal project meeting once a week during the duration of the project. The Contractor shall provide USDA TPMs with Meeting Decision/Action Item Notes within two (2) business days following each weekly meeting.

8. PLACE OF PERFORMANCE

Services may be performed at the vendor corporate offices for non-testing activities. Unless otherwise specified, all testing activities shall occur at the following locations: all work to be performed remotely.

Weekly meeting may be conducted remotely at the discretion of the TPMs.

9. GOVERNMENT FURNISHED FACILITIES/EQUIPMENT

The Government may provide Government Furnished Facilities/Equipment. The Government may provide all required templates and checklist as needed to the vendor(s). The Government may assist the vendor with uploading documentation/information into CSAM which may be made available and used only for tasks related directly to this PWS. The Contractor shall not plug non-GFE equipment into the ARS network. The Government may provide Contractor with assigned and configured RSA Tokens which will assist with remote CSAM entry.

10. PERIOD OF PERFORMANCE

The period of performance under this contract shall be:
ERS Coleridge (formerly NYU ADRF) (ERSNYU): September 1, 2021 to October 31, 2021

The Contractor in coordination with the USDA TPMs/CPB must review Documents thoroughly within the required timeline. However, if corrective work is required to the deliverables, the Contractor is obligated to complete all requirements to satisfaction (deemed by the CPB) not to exceed 45 business days per system, from initial package submission to CPB for Concurrency Review. This means within 45 business days, after initial package submission to CPB for Concurrency Review, the agency has the right to request that the Contractor provide immediate changes/updates (as required by CPB) to documentation regarding

FISMA/USDA policy compliance, at no additional cost. Tasks will **NOT** be considered complete until the system has successfully passed the USDA Concurrency Review.

11. INTELLECTUAL PROPERTY

a. Return of Data

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

b. Release of Information

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

United States Department of Agriculture
Office of Communications
1400 Independence Avenue, SW
Washington, DC 20250

c. Confidentiality and Non-Disclosure

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

The component parts of this effort and reports are expected to contain highly sensitive information that may act as a guide for hostile entities to cause harm to the Department's critical infrastructure. Any such information made available in any format shall be used only for the purpose of carrying out the provisions of this agreement. Such information shall not be divulged or made known in any manner to any person. The Contractor shall immediately notify the Contractor Program Manager, the Contractor on-site Manager, the USDA TPMs and the Contracting Officer upon discovery of any inadvertent disclosures of information. The Contractor shall not retain any information regarding vulnerabilities, to include summaries, the actual vulnerability report, etc., at the end of the task order. All information arising from this task, both hard copy and electronic, shall be returned to the USDA TPMs at task completion.

The Contractor must agree that:

The draft and final deliverables and all associated working papers and other materials deemed relevant by the USDA TPMs that have been generated by the Contractor in the performance of this task order are the property of the U.S. Government and must be submitted to the USDA TPM at the conclusion of the tasks.

All documents produced for this project are the property of the U.S. Government and cannot be reproduced or retained by the Contractor. All appropriate project documentation will be given to the USDA TPM during and at the end of this contract. The Contractor will release no information. Any request for information relating to this Statement of Work presented to the Contractor must be submitted in writing to the USDA TPM and the CO, who in turn will provide a written response. (Contractor employees may be required to sign Non-Disclosure Statements, if necessary, by the agency USDA TPMs.)

d. Sensitive Information Storage and Disclosure

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

Work on this project may require that personnel have access to Privacy Information. Personnel shall adhere to the Privacy Act, Title 5 of the U. S. Code, Section 552a and applicable agency rules and regulations.

The Contractor Program Manager shall ensure that all contract personnel take the required USDA Security Awareness and Rules of Behavior Training.

12. PHYSICAL SECURITY

Contractor custody of sensitive information must be protected under The Privacy Act of 1974, 5 U.S.C. § 552a -- as amended. The Contractor shall be responsible for safeguarding Personally Identifiable Information (PII) data against unauthorized disclosure, dissemination or modification in accordance with the requirements, law and USDA PII policy and regulations. This shall include but is not limited to: Privacy and PII data located in IT Systems, software, research data / information, personnel (institutional knowledge) and buildings/offices.

All contractor personnel who work at USDA must be US Citizens and obtain approval for facility access.

13. PERSONNEL SECURITY REQUIREMENTS

Contractor personnel must comply with USDA Homeland Security Presidential Directive (HSPD-12), “Policy for a Common Identification Standard for Federal Employees and Contractors,” and Federal Information Processing Standards Publication (FIPS PUB) 201, “Personal Identity Verification (PIV) of Federal Employees and Contractors.”

Although the information being processed through this service is not classified, the information is considered highly sensitive PII and must be protected accordingly. It is imperative that company personnel, such as Database Administrators, System Administrators, etc., or anyone who possibly could access the data being processed, have an appropriate level of background investigation on file. The company would be responsible for ensuring that only personnel possessing the appropriate level of background investigation were instrumentally involved with the data processed by this service.

Only US citizens are authorized to work under this contract.

USDA requires government issued identification badges and display of them at all times while on the premises.

Background investigations and fingerprinting are required for all government and Contractor employees. If the government receives an unsuitable report of any Contractor employee after review and processing of security background information, the Contractor will be advised immediately and such employee shall not continue to work at USDA or be assigned work under this or any USDA contract. The Contractor shall replace such employee with a new employee within 30 days.

The Contractor shall ensure that all Contractor employee identification badges are returned to USDA, if employees are dismissed, when the contract expires, or whichever comes first. The Government will have and exercise full and complete control over granting or denying of identification cards or other required security identification badges. It shall be the Contractor's responsibility to account for all identification cards/badges issued to Contractor personnel. Final Contractor payment will be withheld until all identification cards and security identification badges as well as keys or other Government assigned items have been accounted for.

National Agency Check with Inquiries (NACI). The minimum Personnel Security Investigative (PSI) requirements for a Contractor is a NACI. All positions within the USDA are assigned Position Sensitivity Designations (PSDs) based upon the risk/damage an unauthorized disclosure would cause to the Agency and/or National Security. The TPMS will advise the Contractor of the assigned designation and investigative requirements at the kickoff meeting/at the onset of contract discussions. Based upon the assigned sensitivity designation, the minimum level PSI may not meet the requirements and a higher level of investigation and/or Security Clearance may be required.

A list of all Contractor personnel assigned to this task with the dates and types of security background investigation checks completed will be submitted to the TPMS prior to the initiation of any work effort charged against this PWS.

14. KEY PERSONNEL

Technical skills required include a level of expertise in cyber security administration, computer and data networking, as well as experience in support of the national security community, threat and vulnerability assessments and solution design. The Contractor should understand that operational availability is essential when conducting any tests, assessments, reviews, or analysis. In addition, must be fully qualified to conduct any activities as required and hold the appropriate security related certifications.

a. Project Manager

The Contractor shall submit the resumes of its proposed Project Manager and any technical personnel potentially involved in the engagement in their technical proposal. As specified above, all onsite personnel shall have, and be able to provide proof of, an active background investigation clearance.

b. Contractor Personnel Qualifications

Technical skills required include a level of expertise in cyber security administration, computer and data networking, as well as experience in support of the national security community, threat and vulnerability assessments and solution design. The contractor should understand that operational availability is essential when conducting any tests, assessments, reviews, or analysis. In addition, must be fully qualified to conduct any activities as required and hold the appropriate security related certifications.

The Contractor shall submit the resumes of its proposed Project Manager and all key personnel potentially involved with this project along with the proposal. As specified above, all onsite personnel shall have, and be able to provide proof of, an active Federal Government issued clearance.

15. QUALITY CONTROL PLAN – PERFORMANCE-BASED

The Contractor shall provide a Quality Control Plan (QCP) to ensure that the requirements of the contract are met as specified in the Contractor's proposal. This plan shall provide a detailed plan to assure an acceptable quality level is established and maintained. The initial QCP shall be submitted with the Contractor's proposal. The final plan shall be delivered to the USDA TPMs no later than business 5 days after award of the contract. The TPMS will notify the Contractor and Contracting Officer of acceptance or required modifications to the plan before services commence. If changes are needed to the QCP, they shall be completed before the Contractor commences services.

A performance-based Quality Control Plan shall include, but not be limited to the following:

An inspection program addressing the relevant services stated in this PWS. It shall specify the critical quality control points to be inspected on both a schedule and unscheduled basis, and shall include the names, titles and qualifications of the individuals performing the inspections and the extent of their authority. An organizational chart illustrating functional roles will be included in the plan.

Methods of identifying deficiencies in the quality of services performed before the level of performance becomes unacceptable and corrective action is needed; procedures for notifying the COR and USDA TPMs when deficiencies are encountered; planned corrective actions, dates for implementation or completion of correction actions and descriptions of proposed sampling techniques for follow-up inspections. (I.e. a Continuous Improvement Process (CIP).

Methods of documenting and enforcing quality assurance operations of the Contractor's work, including inspection, testing, implementation of corrective actions, and follow-up inspections.

The format for the Contractor's Quality Assurance Report.

The Contractor, throughout the term of the contract shall maintain documentation of all quality control inspections, inspection results, and corrective actions required and performed. This documentation will be included in the quarterly activity report as described in Section 10.0, Key Deliverables, and Quality Control Plan.

Performance standards are an essential measure of contractor performance. Standards should be designed and met in such a manner as to assure quality. To this end, ERS will monitor the quality of the contractor performance. This monitoring has two aspects that will meet the needs of the ERS Quality Assurance Monitoring and Quality Assurance Review. All items listed below (in Section 10.0) are measurable and are in accordance with this PWS.

16. KEY DELIVERABLES

a. RMF Steps 1-3b Key Deliverables

ITEM	DELIVERABLE / EVENT	OBJECTIVE	DUE BY
1	Kick-Off Meeting	Introductions and discussions to include implementation strategy, confirm assumptions with USDA staff, and build the statement of the project's vision. See Task 4.1.3	No Later Than 5 business days after date of award
2	Proposed Project Plan	Proposed plan to define responsibilities, timelines, deliverables, risks, and milestones necessary to accomplish the objectives of contract. See Task 4.1.3	Due with proposal – will be discussed at the Kick-Off Meeting.
3	Final Project Plan	See Task 4.1.3	Not Later Than 5 business days after Kick-off Meeting.
4	Weekly Status Reports	See Task 4.1.4	Due Friday of each week
5	Weekly Status Meetings and Oral Briefings/Presentations.	See Task 4.1.5	Due Wednesday of each week
6	Proposed Quality Control Plan	See Paragraph 9.0	Due with proposal
7	Final Quality Control Plan	See Paragraph 9.0	Not Later Than 5 business days after Kick-off Meeting.
8	Final Quality Control Plan	See Paragraph 9.0	Not Later Than 5 business days after Kick-off Meeting.
9	Concurrency Review and CPO Acceptance (Concurrence /Approval Memorandum).	See Paragraph 1.4	Not Later Than 45 business days after contract award.
10	Conflict of Security Interest & Disclosure	See Paragraph 4.0, Paragraph 12 and	Due with proposal

		Attachment 2	
11	USDA Security Awareness and Rules of Behavior Training	See Paragraph 6.3	Not later than 45 business days after Kick-off Meeting or as agreed by TPMS.
12	Form NFC-1267-C, Contractor Separation Clearing Report, if applicable	See Paragraph 8.11	Within the timeframes as stated in Title VII, Chapter 8, Directive 12, Separation Clearing Report for Contractor Personnel.
13	Release of Claim & Contract Completion Statement	See Paragraph B, Paragraph J, and Attachment 3.	Submit with final invoice. Contractor must obtain signature from TPMS, prior to submission.

17. GENERAL REQUIREMENTS

The Contractor shall provide all personnel and services necessary to support the USDA in accordance with this PWS.

a. Performance Requirements

This contract is for performance-based services. The Contractor shall provide performance reports as specified in 16.0, Key Deliverable Schedule. The COR and USDA TPMs will monitor the Contractor's performance under this contract in accordance with the defined procedures, methods and guidelines. The COR and USDA TPMs will examine both timeliness and quality aspects of the Contractor's performance.

The COR and USDA TPMs are required to inform the Contracting Officer immediately of any issues such as unsatisfactory documents to reach an immediate solution. The Contractor shall inform the COR and USDA TPMs if required deadlines will not be met. Weekly meetings and status reports are required in this process.

b. Performance Standards

The Performance Standards utilized in this contract include:

- Timeliness & Accuracy of Delivery and Performance
- Customer Satisfaction & Account Representative Support
- Physical and Personnel Security
- Personnel – Continuity of Services
- Contractor Reports and Data Files (Timeliness & Quality)
- Conflict of Security Interest & Disclosure

c. Performance Expectations

Two levels of performance are specified. A brief discussion of each level follows:

a. Performance Level 1 (Acceptable). This is the level of performance is acceptable and is expected from the Contractor during each performance period.

b. Performance Level 2 (Unacceptable). This level of unacceptable performance is where the Contractor's performance is deficient. The Contractor will be allowed a period not to exceed 10 calendar days to correct Performance Level 2. The Contractor must prepare a written improvement plan and the performance must be improved within 10 calendars day or the Contractor may be subject to deductions and/or termination procedures.

Performance at level 2 for any one-week will require that the Contractor provide a written improvement plan and the details will be documented on the weekly status report. Upon TPMS review and approval of this improvement plan, the Contractor will have up to 10 calendar days to return to Performance Level 1. If Performance Level 2 (Unacceptable) is not improved the Contractor shall be: 1) subject to additional meetings; 2) subject to the Government obtaining services elsewhere and actual cost of services deducted from the Contractor's invoice covering the period for which the outside services were obtained (Contractor responsible for reimbursement of these costs); and 3) subject to payment deductions as outlined in Technical Exhibit 1 for the next invoice(s). The deduction for less than acceptable performance will be deducted the second month following the formal evaluation/status meeting. See Technical Exhibit 1, Performance Requirements Summary. The Contractor may also be subject to contract termination for default, if one (1) performance standard is at Performance Level 2 (Unacceptable) for two (2) months or if two (2) or more performance standards are at Performance Level 2 (Unacceptable) for two (2) months.

d. Performance Evaluation Meetings

The Contractor shall schedule and meet with the USDA TPMs weekly until the service is fully implemented into production. Thereafter, these meetings shall be held as often as deemed necessary by the USDA TPMs or the Contracting Officer. At these meetings a mutual effort will be made to resolve any concerns which have been identified. Any performance evaluations and assessments should be discussed, and all meetings shall be documented.

The Contractor shall prepare and provide written minutes of meetings, which will be discussed and approved by the USDA TPMs/designated representative for signature. If the COR/USDA TPMs or their designated representative does not concur with any portion of the minutes, notice of such non-concurrence will be provided to the Contractor within five (5) business days following receipt of the minutes. The Contractor shall acknowledge and resolve all disputes and resubmit the minutes to the COR/USDA TPMs or their designated representative within five (5) business days of receipt of the USDA's non-concurrence.

e. Contractor Performance Assessments

Assessments. USDA may do assessments of the Contractor's performance. Contractor will have an opportunity to respond to assessments, and independent verification of the assessment may be utilized in the case of disagreement.

Record. Completed assessments may be kept on record at USDA ERS and may serve as past performance data. Past performance data will be available to assist agencies in the selection of IT service providers for future projects. Past performance data may also be utilized in future procurement efforts.

f. SECTION 508 - ACCESSIBILITY OF ELECTRONIC AND INFORMATION TECHNOLOGY

(a) This Performance Work Statement (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 (P.L. 105-220). Specifically, subsection 508(a)(1) requires that when the Federal Government procures Electronic and Information Technology (EIT), the EIT must allow Federal employees and individuals of the public with disabilities comparable access to and use of information and data that is provided to Federal employees and individuals of the public without disabilities.

(b) The EIT accessibility standards at 36 CFR Part 1194 were developed by the Architectural and Transportation Barriers Compliance Board ("Access Board") and apply to contracts and task/delivery orders, awarded under indefinite quantity contracts on or after June 25, 2001.

(c) Each Electronic and Information Technology (EIT) product or service furnished under this contract shall comply with the Electronic and Information Technology Accessibility Standards (36 CFR 1194), as specified in the contract, as a minimum. If the Contracting Officer determines any furnished product or service is not in compliance with the contract, the Contracting Officer will promptly inform the Contractor in writing. The Contractor shall, without charge to the Government, repair or replace the non-compliant products or services within the period of time to be 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:

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

(d) The contractor must ensure that all EIT products that are less than fully compliant with the accessibility standards are provided pursuant to extensive market research and are the most current compliant products or services available to satisfy the contract requirements.

(e) For every EIT product or service accepted under this contact 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.

i. Section 508 Compliance for Communications

The Performance Work Statement (PWS) 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.
Rehabilitation Act, Section 508 Accessibility Standards

1. 29 U.S.C. 794d (Rehabilitation Act as amended)
2. 36 CFR 1194 (508 Standards)
3. www.access-board.gov/sec508/508standards.htm (508 standards)
4. FAR 39.2 (Section 508)

ii. USDA Standards, policies and procedures (Section 508)

In addition, all contract deliverables are subject to these 508 standards as applicable.
Regardless of format, all Web content or communications materials produced, including text, audio or video - must conform to applicable Section 508 standards to allow federal employees and members of the public with disabilities to access information that is comparable to information provided to persons without disabilities. All contractors (including subcontractors) or consultants responsible for preparing or posting

content must comply with applicable Section 508 accessibility standards, and where applicable, those set forth in the referenced policy or standards documents above. Remediation of any materials that do not comply with the applicable provisions of 36 CFR Part 1194 as set forth in the SOW, PWS, or TO, shall be the responsibility of the contractor or consultant.

The following Section 508 provisions apply to the content or communications material identified in this PWS:

- 36 CFR Part 1194.21 a - l
- 36 CFR Part 1194.22 a - p
- 36 CFR Part 1194.31 a - f
- 36 CFR Part 1194.41 a – c

The contractor shall provide a completed Section 508 Product Assessment Template and the contractor shall state exactly how proposed EIT deliverable(s) meet or does not meet the applicable standards.

The following Section 508 provisions apply for software development material identified in this PWS:
For software development, software applications, and operating systems the Contractor/Developer/Vendor shall comply with the standards, policies, and procedures below:

Rehabilitation Act, Section 508, Accessibility Standards
(1) 29 U.S.C. 794d (Rehabilitation Act as amended)
(2) 36 CFR 1194 (508 Standards)
36 CFR Part 1194.21 (a – l)
36 CFR Part 1194.31 (a – f)
36 CFR Part 1194.41 (a – c)
(3) www.access-board.gov/sec508/508standards.htm (508 Standards)
(4) FAR 39.2 (Section 508)
(5) USDA Standards, policies and procedures (Section 508)
a. Information Technology – General Information
http://www.ocio.usda.gov/508/index.html#resources

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

Rehabilitation Act, Section 508, Accessibility Standards
(1) 29 U.S.C. 794d (Rehabilitation Act as amended)
(2) 36 CFR 1194 (508 Standards)
36 CFR Part 1194.22 (a – p)
36 CFR Part 1194.31 (a – f)
36 CFR Part 1194.41 (a – c)
(3) www.access-board.gov/sec508/508standards.htm (508 Standards)
(4) FAR 39.2 (Section 508)
(5) USDA Standards, policies and procedures (Section 508)
a. Information Technology – General Information
http://www.ocio.usda.gov/508/index.html#resources

For Telecommunication products the Contractor shall comply with the standards, policies, and procedures below:

Rehabilitation Act, Section 508, Accessibility Standards

(1) 29 U.S.C. 794d (Rehabilitation Act as amended)
(2) 36 CFR 1194 (508 Standards)
36 CFR Part 1194.23 (a – k)
36 CFR Part 1194.31 (a – f)
36 CFR Part 1194.41 (a – c)
(3) www.access-board.gov/sec508/508standards.htm (508 Standards)
(4) FAR 39.2 (Section 508)
(5) USDA Standards, policies and procedures (Section 508)
a. Information Technology – General Information
http://www.ocio.usda.gov/508/index.html#resources

For video and multimedia applications (including training), the Contractor shall comply with the standards, policies, and procedures below:

Rehabilitation Act, Section 508, Accessibility Standards

(1) 29 U.S.C. 794d (Rehabilitation Act as amended)
(2) 36 CFR 1194 (508 Standards)
36 CFR Part 1194.24 (a – e)
36 CFR Part 1194.31 (a – f)
36 CFR Part 1194.41 (a – c)
(3) www.access-board.gov/sec508/508standards.htm (508 Standards)
(4) FAR 39.2 (Section 508)
(5) USDA Standards, policies and procedures (Section 508)
a. Information Technology – General Information
http://www.ocio.usda.gov/508/index.html#resources

For self-contained, closed products, the Contractor shall comply with the standards, policies, and procedures below:

Rehabilitation Act, Section 508, Accessibility Standards

(1) 29 U.S.C. 794d (Rehabilitation Act as amended)
(2) 36 CFR 1194 (508 Standards)
36 CFR Part 1194.25 (a – j)
36 CFR Part 1194.31 (a – f)
36 CFR Part 1194.41 (a – c)
(3) www.access-board.gov/sec508/508standards.htm (508 Standards)
(4) FAR 39.2 (Section 508)
(5) USDA Standards, policies and procedures (Section 508)
a. Information Technology – General Information
http://www.ocio.usda.gov/508/index.html#resources

For Desktop and portable computers, the Contractor shall comply with the standards, policies, and procedures below:

Rehabilitation Act, Section 508, Accessibility Standards

(1) 29 U.S.C. 794d (Rehabilitation Act as amended)
(2) 36 CFR 1194 (508 Standards)
36 CFR Part 1194.26(a – d)
36 CFR Part 1194.31 (a – f)
36 CFR Part 1194.41 (a – c)
(3) www.access-board.gov/sec508/508standards.htm (508 Standards)
(4) FAR 39.2 (Section 508)
(5) USDA Standards, policies and procedures (Section 508)
a. Information Technology – General Information
http://www.ocio.usda.gov/508/index.html#resources

All Electronic Information Technology that is subject to the 36 CFR 1194 standards will have a Section 508 acceptance test and Section 508 will be validated upon acceptance.

All maintenance for Electronic Information Technology that requires upgrades, modifications, installations and purchases will adhere to the Section 508 Standards and 36 CFR 1194.

ATTACHMENT 2
CONFLICT OF SECURITY INTEREST & DISCLOSURE
RISK MANAGEMENT FRAMEWORK
ERS Coleridge (NYU ADRF)

Contractor #: ___________________
Contractor Name: __________________
Contractor Address: _________________
Contact Name: ______________________
Telephone: ____________________
Email: ______________________

The BPA Contractor that perform RMF Step 1-3b must not perform RMF Step 4-4b on the **ERS Coleridge (NYU ADRF)** system and vice versa.

The Contractor must certify that they have not performed RMF Step 4-4b on the **ERS Coleridge (NYU ADRF)** system within the same accreditation cycle. Attachment 2, Conflict of Security Interest and Disclosure must be completed and submitted with the Contractor's proposal.

Performing both RMF Step 1-3b and RMF Step 4-4b on the **ERS Coleridge (NYU ADRF)** system within the same accreditation cycle violates USDA (OIG,OCIO-CPO) accepted best practices to ensuring independence and separation of duties. Violations may result in contract termination. The Government may take additional actions, as well. The same Contractor cannot perform both RMF Step 1-3b and RMF Step 4-4b regardless of the FIPS199 (Low, Moderate or High).

The Contractor shall disclose the name of all USDA systems, USDA agency names and dates they performed SA&A on each system.

a. Risk Management Framework (RMF) Step 1-3b, (Formerly C&A Phase 1)

System Name	Date Completed Concurrency Review	Agency	Call Order#

b. Risk Management Framework (RMF) Step 4-4b, (Formerly C&A Phase 2)

System Name	Date Concurrency Review Completed	Agency	Call Order#

_________________________________ ________________
(Print Name and Sign) (Date)

Note: The Contractor must complete and submit Attachment 2 with each proposal for service. See PWS, Paragraph 3.0, Scope of Work, Conflict of Security Interest and Disclosure for additional information.