A Statement of Work (SOW) is typically used when the task is well-known and can be described in specific terms. Statement of Objective (SOO) and Performance Work Statement (PWS) emphasize performance-based concepts such as desired service outcomes and performance standards. Whereas PWS/SOO's establish high-level outcomes and objectives for performance and PWS's emphasize outcomes, desired results and objectives at a more detailed and measurable level, SOW's provide explicit statements of work direction for the contractor to follow. However, SOW's can also be found to contain references to desired performance outcomes, performance standards, and metrics, which is a preferred approach.

The Table of Content below is informational only and is provided to you for purposes of outlining the PWS/SOO/SOW. This sample is not all inclusive, therefore the reader is cautioned to use professional judgment and include agency specific references to their own PWS/SOO/SOW.

STATEMENT OF WORK

Project Name & ID: _____

May 1, 2011

1.0 SCOPE

Provide the expertise, technical knowledge, staff support, and other related resources necessary to:

- Perform analysis to ensure security controls are consistently implemented.
- Integrate new technology with IT security standards.
- Develop and execute plans for monitoring, assessing and verifying security controls across all major information systems.
- Develop, evaluate, and exercise IT survivability and contingency plans.

1.1 BACKGROUND / CURRENT CONTRACT ENVIRONMENT

As the agency moves forward to meet the security mandates required by federal laws, standards, and guidance, a more advanced conceptual and continuous approach to security will be required to ensure the safeguarding of information entrusted to the agency. This "Comprehensive and Robust" Information Security Program can be accomplished: (1) by continuing to implement and update NIST-compliant policies, and procedures, (2) by engineering and implementing solutions to new requirements that arise both from advances in technology and from new Federal and regulations and directives and (3) by maintaining IT system resiliency with effective contingency planning, evaluation, and testing.

1.2 OBJECTIVES

The following are objectives of the CRIS program:

- Perform gap analysis on current security infrastructure
- Ensure consistent application of information security standards across all agency information systems.
- Meet all regulatory and agency documented standards and guidance.
- Integrate these regulations and standards into a fully implementable security program.
- Ensure preparation for internal and external audits through management of all infrastructure artifacts required to pass audits.
- Ensure all new information technology (IT) projects meet or integrate security standards into their development.
- Develop a culture of security-mindful professionals across the community.
- Strive to be more flexible and responsive to new regulatory directives.
- Serve as the central authority for all IT security-related activities across the agency.
- Ensure information system survivability and integrity.
- Optimize processes to meet IT security-related goals and strategies

1.3 APPLICABLE DOCUMENTS

1.4 DEFINITIONS

2.0 STATEMENT OF WORK (SOW)

2.1 TASK MANAGEMENT

The Contractor shall provide sufficient management to ensure that these tasks are performed efficiently, accurately, on time, and in compliance with the requirements of this document. Specifically, the Contractor shall designate a single manager to oversee these tasks and supervise staff assigned. The Contractor shall ensure that a monthly performance and progress report is submitted outlining the expenditures, billings, progress, status, and any problems/ issues encountered in the performance of these tasks.

2.1.1 Monthly Performance and Progress Report (MPPR)

The Contractor shall ensure that a MPPR is submitted outlining the expenditures, billings, progress, status, and any problems/ issues encountered in the performance of this task.

The MPPR shall also include the labor hours expended, by labor category, for each task and sub-task.

The Contractor shall submit the MPPR within ten (10) calendar days after the end of reporting period.

2.1.2 Program Management Plan (PMP)

The Contractor shall develop PMP that shall require Government approval. A draft shall be submitted with the technical and cost proposals for this PB SOW. The PMP will be used to manage, track and evaluate the Contractor's performance. The PMP shall consist of control policies and procedures in accordance with standard industry practices for project administration, execution and tracking.

The Program Management Plan shall be due fifteen (15) calendar days after the effective date of award.

2.1.2 Quality Assurance Plan (QAP)

The Government and the Contractor shall jointly cooperate in the development and implementation of a QAP. A draft shall be submitted with the technical and cost proposals for this PB SOW. Once approved, the QAP becomes final and unless modified, governs all QA procedures for the balance of the contract performance. The final QAP shall be submitted fifteen (15) calendar days after period of performance start date.

The QAP shall document the process that will verify and validate quality assurance in compliance with the contract requirements and ensure these requirements meet the Government's expectations. This QAP shall consist of a Government approved QA process, periodic quality briefings within the Interim Progress Review (IPR) process, and Government surveillance.

The Contractor shall develop a QAP that provides for the monitoring of the quality of the services, work products, and deliverables required under the contract. The Contractor shall develop the QAP based on accepted industry standards such as the CMMI SM, ISO 9000 IEEE 12207, or other accepted industry QA standards. The QAP shall detail the processes, procedures, and metrics for assuring quality. The QAP shall also include, at a minimum, a description of the following key activities:

- Establishment of capable processes;
- Monitoring and control of critical processes and product variation;
- Establishment of mechanisms for feedback of field performance;

- Implementation of an effective root cause analysis and corrective action system; and
- Continuous process improvement.

During performance of the contract, the Contractor shall maintain a QA inspection system that contains procedures and processes that are consistent with the monitoring and control processes identified in the approved QAP.

The final, approved QAP shall provide for the Contractor to conduct periodic briefings to the Government within the IPR process. Prior to the IPR briefing the Contractor shall document the root cause of the problem and provide a description of the corrective action taken (or being taken). The corrective action shall be consistent with the Contractor's continued process improvement and field feedback mechanisms identified in the approved QAP.

The Contractor shall maintain records documenting all corrective actions and process improvements undertaken during contract performance. The records shall validate the Contractor's compliance with the processes contained in the QAP. The Contractor shall make the records available to the Government during contract performance and for a period of five (5) years after final payment under the contract.

The Government has the right to perform periodic surveillance of the Contractor to assure that the Contractor's work products and QA processes are in compliance with the contract requirements. The Government and the Contractor will coordinate Government surveillance in a manner that will not unduly delay or disrupt the Contractor's performance of the contract.

2.1.4 Management Briefing Support

The Government will conduct semi-annual Integrated Progress Reviews (IPRs). The IPR shall address, at a minimum, the following:

- Progress and status of all activities,
- Milestones and achievements,
- Schedule and financial risks,
- Cost status of all activities by task, and
- Schedule status of all activities.

As required, the Contractor shall assist the Government in preparing and briefing the IPR.

2.2 ADDITIONAL TASKS

The following tasks are included in the base task list or listed as optional tasks:

- Base Task Area 2.2.1: Enterprise Security Program Guidance and Policy Management
- Base Task Area 2.2.2: Oversight and Compliance Verification
- Base Task Area 2.2.3: Survivability and Contingency Program Support
- Base Task Area 2.2.4: Certification and Accreditation Coordination
- Base Task Area 2.2.5: Enterprise Security Metric Reporting
- Base Task Area 2.2.6: Information Security Outreach and Awareness
- Optional Task Area 2.2.7: Vulnerability Scanning and Auditing
- Optional Task Area 2.2.8: Security Program Assessment Support
- Optional Task Area 2.2.9: Centralized Account Management
- Optional Task Area 2.2.10: Technical Approval Support

- Optional Task Area 2.2.11: IT Security Process Improvement
- Optional Task Area 2.2.12: Wireless Network Security Assessment
- Optional Task Area 2.2.13: Network Security Assessment
- Optional Task Area 2.2.14: Program Support to FS IT Security Program

BASE Task 2.2.1 – Enterprise Program Guidance and Policy Management

Subtask 2.2.1.1 - Security Documentation Management and Governance

- Evaluate and recommend an enterprise-wide security document management solution and methodology. If implemented, support and maintain the document management solution.
- Provide expert analysis of new federal guidance and/or changes to the security environment as it impacts security documentation.
- Support and maintain the confidentiality, integrity, and availability of security documentation.
- Optimize the content and usability of policy- and procedure-related security documentation
- Perform annual review and recommend updates of the Manual 6680 policy section
- Perform annual review and recommend updates of up to 125 enterprise-wide IT security procedures within 11 months of last government approval date
- Perform periodic testing and evaluation of the effectiveness of information security policies, procedures, practices, and security controls to be performed with a frequency depending on risk, but no less than annually

Subtask 2.2.1.2- Regulatory and Legislative Analysis

- Track and analyze new legislative, Office of Management and Budget (OMB), National Institute of Standards and Technology (NIST), and agency requirements.
- Based on the analysis and anticipated impacts, develop security recommendations tailored to agency needs.

Subtask 2.2.1.3- Risk Management Framework and Strategy

Effective management of risk from information systems involves the following key elements:

- Assignment of information security responsibilities to senior leaders/executives within the organization;
- Understanding by senior leaders/executives of the degree of protection or risk mitigation that implemented security controls provide against today's sophisticated and diverse threats;
- Recognition and acceptance by senior leaders/executives of the risks (including potential magnitude of harm) to organizational operations and assets, individuals, other organizations, and the Nation arising from the use of information systems; and
- Accountability by senior leaders/executives for their risk management decisions.

Managing that portion of organizational risk related to information systems begins with an effective information security program and a risk management strategy. The tasks for the development of the risk management strategy and Framework are:

- Provide recommendations for comprehensive strategy to manage risk to organization and assets
- Provide a concept of operations for evaluating risk across the agency with respect to risk tolerance
- Recommend risk executive function to facilitate consistent, agency-wide application of the risk management strategy
- Develop a plan for implementation of a Risk Management Framework and assist in implementation
- Provide an annual update of the Agency Risk Management Framework

Subtask 2.2.1.4 – Information Security Program Plan

- Compile documents that will be used in the formation of the Information Security Program Plan
- Develop an Information Security Program Plan
- Provide an annual update of the Information Security Program Plan

Base Task 2.2.2 - Oversight and Compliance Verification

Subtask 2.2.2.1 - OMB Circular A-123 Assessment and Continuous Monitoring

- Provide support for verifying compliance with OMB Circular A-123.
- Develop and execute test plans of the OMB Circular A-123 internal control assessments for up to 40 information technology systems for up to 70 controls annually.
- Determine, gather, examine, and analyze artifacts related to OMB Circular A-123 security control assessments and remediation verification.
- Enter test results and artifacts into the agency repository.
- Document assessment activities and results in sufficient detail to enable external review of all assessment processes, activities, results, and conclusions.
- Support agency A-123 Team review of assessment activities, reports, and conclusions.
- Provide recommendations and guidance for corrective action of all non-compliant security controls.
- Provide security expertise to ensure security controls are implemented and the resulting documentation and artifacts are current.
- Provide guidance to key stakeholders on the necessary components to demonstrate the achievement of control objectives.
- Design, develop, and implement a NIST-compliant continuous monitoring process across all major information systems to provide periodic assurance to senior management on the security protections of

major information systems.

- Support periodic assessment of a agency-identified subset of security controls across all major information systems.

Subtask 2.2.2.2– IT Security Support to Data Center Migration

- Provide security support for the Application/Data Center Migration Effort to consolidate up to 125 regional applications/tables per year.
- Assist in identification of applications/tables in the FS environment to be migrated to FS Data Centers
- Characterize applications/tables as a minor application, major application or neither (more like a utility, not an application)
- Categorize applications according to FIPS 199, Standard for Security Categorizations of Federal Information and Information Systems
- Provide certification and accreditation (C&A) expertise in the application of best practices to the bundling of applications for C&A purposes, ensuring compliance with both federal and agency requirements.
- Maintain and provide reports on the C&A status of application migration and supporting documentation.

Base Task 2.2.3 – Survivability and Contingency Program Support

Subtask 2.2.3.1 – Contingency Plan Development and Evaluation

- Develop and/or revise Business Impact Analysis (BIAs) to include business process, IT dependency, and physical security assessments for headquarters units, 9 Regional Offices, 7 Stations and 1 Area headquarters offices, Albuquerque Service Center, and IT facilities located nation-wide.
- Utilize virtual means, where practical, to collect BIA data to include, but not limited to survey forms, telephone calls, and electronic mail.
- Develop annual BIA program of work plan and schedule based on age of previous documents. A three year update cycle of previous BIAs is anticipated. One third of approximately 40 existing BIAs are to be updated each year.
- Conduct and/or revise one third of approximately 40 existing physical security assessments at proposed or existing major data center sites.
- Compile and/or revise annual aggregated BIA crosswalk report summarizing BIA work for the year and supporting presentation material.
- Perform annual review and analyze up to 40 IT contingency plans (ITCPs) and disaster recovery plans (DRPs) for NIST, USDA, and FS standards compliance to produce checklists for IT systems.
- Assist with formulation and annual update of the nation-wide IT Continuity of Operation Plans (COOP), Crisis Management Plan (CMP), Communication and other contingency documents or plans.
- Produce draft and final versions of all reports and documents for government review and comment.

Subtask 2.2.3.2 – Contingency Plan Exercise and Training

- Conduct and document semi-annual notification drills for up to 40 IT system ITCPs and DRPs. One drill to be conducted in the spring and the second in late fall of each calendar year.
- Conduct and document annual table top exercise or all IT systems ITCP and DRPs during the winter of each calendar year for up to 40 IT systems.
- Observe and document tabletop and/or functional COOP exercises at nation-wide headquarter locations for up to four locations each calendar year.
- Conduct and document bi-annual table top and/or functional COOP exercise for the enterprise level IT leadership and personnel.
- Assist with exercise and/or training and documentation of nation-wide IT COOP, CMP, Communication and other contingency documents or plans.
- Produce test plans, draft after actions, final after actions, and other documents for government review and comment.

Base Task 2.2.4 – Certification and Accreditation Coordination

- Conduct Certification and Accreditation (C&A) package reviews for General Support Systems to ensure compliance with all federal, and agency requirements for up to 3 General Support Systems per calendar year.
- Prepare and/or revise C&A packages of application systems for review for up to 15 IT systems per calendar year.
- Review and/or revise all C&A supporting documentation to ensure consistency across interrelated C&A package components including required revisions in CSAM database.
- Provide security expertise and guidance to ensure the consistent application of C&A processes across all major information systems.
- Maintain and provide reports on the status of all C&A materials and supporting documentation.
- Provide C&A expertise in the application of best practices to standardize and enhance C&A processes, ensuring compliance with both federal and USDA requirements.

Base Task 2.2.5 – enterprise Security Metric Reporting

- Provide ongoing awareness of relevant security issues and threats.
- Develop security metrics to demonstrate security efficacy.
- Implement web-based reporting tool for displaying metrics.

Base Task 2.2.6 – Information Security Outreach and Awareness

- Analyze and evaluate the communities within agency to tailor security-related communication messages.
- Develop and implement an outreach program to ensure continuous awareness of relevant security environmental conditions throughout the FS community.
- Maintain and execute a comprehensive security communications and training plan.

Optional Task 2.2.7 – Vulnerability Scanning and Auditing

- Perform enterprise-wide internal and external vulnerability testing and scanning monthly to assess the agency security posture using Foundstone and NESSUS
- Prepare report on scanning results monthly
- Perform enterprise-wide detection of server configuration changes using Tripwire
- Prepare a report monthly of analysis of security configuration management

Optional Task 2.2.8 - Security Program Assessment Support

- Provide plan for assessing the performance of the Security Program using the methodology specified in NIST NISTIR 7358 or other similar methodology specified including:

    1. Develop project plan for Security Program assessment.
    2. Determine, gather, examine, and analyze artifacts related to Security Program assessment and external audits.
    3. Document assessment activities and results in sufficient detail to enable external review of all assessment processes, activities, results, and conclusions.
    4. Provide recommendations and guidance for Security Program improvements and corrections.

Optional Task 2.2.9- Centralized Account Management

- Provide an assessment of the technical requirements and guidelines of centralized account management including review of the consistent management of user, privileged, and system accounts.
- Provide plan for the improvement of user, privileged, and system centralized account management.

Optional Task 2.2.10- Technical Approval Support

- Evaluate up to 10 technical approval requests a week for 3 months to determine security risks and implications of new IT procurement.

- Provide formal evaluation responses and recommendations for technical approval requests.

Optional Task 2.2.11- IT Security Process Improvement

- Provide recommendation for improvement of the Security processes and procedures including but not limited to:

    1. Identify and analyze existing IT Security processes and procedures within the agency to meet new IT Security goals and objectives
    2. Optimize underlying processes to achieve more efficient results
    3. Align the agency business processes to realize IT Security goals

Optional Task 2.2.12 – Wireless Assessment

- Conduct security testing and develop assessment of wireless local area networks (WLANs) and their components to ensure compliance with current security guidelines and requirements

Optional Task 2.2.13 – Network Security Assessment

- Conduct security testing and develop assessment of local area networks (LANs) and their components to ensure compliance with current security guidelines and requirements

Optional Task 2.2.14 - Provide Program Support to the IT Security Program

As a natural outgrowth of the work described in Subtasks 2.2.1 through 2.2.6, the Government would require additional support services from the contractor. Possible work may include having the contractor assist in IT security program implementation specific to additional information systems but are not limited to the following:

- Communicate project information and deliverables to the project team, to the project stakeholders, and to affected IT staff
- Maintain web site information and team room about project status
- Write and provide weekly interim status report to outline all active projects within each task area.
- Collect and document project deliverables and marshal them for the agency and OIG review
- Develop concept of operations and strategy documents
- Develop self-help documentation/training materials i.e. cheat sheets for procedures.
- Develop methods and media for communication and education, including relevant security awareness and training programs, to ensure the consistent application of security policy and procedures.
- Support security initiatives with communication planning and execution.
- Facilitate information security implementation workshops and conferences.

3.0 INSPECTION AND ACCEPTANCE

The Contracting Officer's Representative (COR) for the Task Order is responsible for inspection and acceptance of all services, incoming shipments, documents, and services.

3.1 ACCEPTANCE CRITERIA

Certification by the Government of satisfactory services provided is contingent upon the Contractor performing in accordance with the terms and conditions of the referenced agreement, this order, and all amendments.

3.2 CONTRACTOR PAYMENT PROCESSING

The Contractor is responsible for properly preparing, and forwarding to the appropriate Government official, the invoice and receiving report for payment. The Contractor shall invoice in accordance with Section B of the task order. All Other Direct Costs (ODCs) exceeding $2500 requires that the Contractor conduct appropriate competition.

3.3 INVOICE REVIEW

The COR may reject or require correction of any deficiencies found in the invoice or receiving report. In the event of a rejected invoice or receiving report, the Contractor must be notified in writing by the COR of the specific reasons for rejection.

4.0 DELIVERABLES

4.1 DELIVERY ADDRESS

The Contractor shall submit all deliverables to COR at the following address:

Should the size of a Deliverable require that it be placed upon a CD, the Contractor shall prepare and deliver to the CDRL support center an individual envelope for each addressee. As appropriate, this envelope shall contain one or more CDs. Other recipient's addresses are located in Section 5.0.

4.2 METHOD OF DELIVERY

Electronic copies shall be delivered using Microsoft Office suite of tools (for example, MS WORD, MS EXCEL, MS POWERPOINT, MS PROJECT, or MS ACCESS format), unless otherwise specified by the COR-DO. Electronic submission shall be made via email, unless otherwise agreed to by the COR-DO.

4.3 GOVERNMENT ACCEPTANCE PERIOD

The COR-DO will have fifteen (15) workdays to review draft deliverables and make comments. The Contractor will have five (5) workdays to make corrections. Upon receipt of the final deliverables, the COR will have five (5) workdays for final review prior to acceptance or providing documented reasons for non-acceptance. Should the Government fail to complete the review within the review period the deliverable will become acceptable by default.

The COR will have the right to reject or require correction of any deficiencies found in the deliverables that are contrary to the information contained in the Contractor's accepted proposal. In the event of a rejected deliverable, the Contractor will be notified in writing by the COR of the specific reasons for rejection. The Contractor shall have five (5) workdays to correct the rejected deliverable and return it per delivery instructions.

4.4 DELIVERABLE/DELIVERY SCHEDULE

SOW Task#	Title	Format	Distribution	Frequency and Remarks
6.2.6	Non-Disclosure agreement	Contractor-Determined Format	Standard Distribution	Signed statements are due, from each employee assigned, *prior to* performing *ANY* work on this task.
2.1.1	Monthly Performance and Progress Report	Contractor Determined Format	Standard Distribution	NLT 10th of each reporting period.
2.1.3	Program management plan	Contractor Determined Format	Standard Distribution	NLT 15 calendar DACA and updates as requested by COR
2.1.4	Quality Assurance Plan (QAP)	Contractor Determined Format	Standard Distribution	NLT 15 calendar DACA and updates as requested by COR
2.2.1.1	Security documentation system recommendation	Contractor Determined Format	Standard Distribution	NLT 120 calendar DACA
2.2.1.1	Gap Analysis on procedures against policies and procedures	Contractor Determined Format	Standard Distribution	Analysis provided by January 15
2.2.1.1	Procedure Effectiveness Measurement	Contractor Determined Format	Standard Distribution	Report provided by August 1
2.2.1.1	Annual Procedure currency Review	Contractor Determined Format	Standard Distribution	Reviews submitted within 11 months of government's last procedure approval date
2.2.1.1	Updated Policy recommendations	Contractor Determined Format	Standard Distribution	Policy review submitted by November 1
2.2.1.2	New regulation recommendations	Contractor Determined Format	Standard Distribution (*)	Recommendation within 60 days of issuance
2.2.1.3	Risk Management Strategy and CON-op recommendation	Contractor Determined Format	Standard Distribution	Final Strategy developed with 60 days of task order award and ConOps developed within 60 days of approved strategy
2.2.1.3	Risk Management Framework Strategy and Implementation Plan	Contractor Determined Format	Standard Distribution	Plan developed within 60 days of approved ConOps, annual update due by September 30
2.2.1.4	Information System Security Plan / Update	Contractor Determined Format	Standard Distribution (*)	Final Program Plan developed within 120 calendar DACA, Update due by July 30
2.2.2.1	A-123 Test Plan Development	Contractor	Standard	Plans, assessments, and

		Determined Format	Distribution	reports developed, reviewed, completed and reported in CSAM by May 1
2.2.2.1	A-123 Test control assessment documentation and compliance data entry in CSAM	Contractor Determined Format	Standard Distribution	Plans, assessments, and reports developed, reviewed, completed and reported in CSAM by May 1
2.2.2.1	Continuous Monitoring Plan	Contractor Determined Format	Standard Distribution	Plan developed, reviewed and implemented within 180 days of task order award
2.2.2.1	Corrective Action Plan Recommendation	Contractor Determined Format	Standard Distribution	Recommendation developed by June 15
2.2.2.2	Application Security Categorizations	Contractor Determined Format	Standard Distribution	Categorizations and results developed within 90 days after task order award for every lot of 25 migrations
2.2.2.2	Application Migration Status Reports	Contractor Determined Format	Standard Distribution	NLT 10th of each reporting period.
2.2.3.1	Business Impact Assessments	Contractor Determined Format	Standard Distribution (**)	Final BIAs and physical security assessments provided within 90 days of onsite review
2.2.3.1	Program of Work for BIAs	Contractor Determined Format	Standard Distribution	POW for BIAs provided due Nov 1
2.2.3.1	Physical Security Assessments	Contractor Determined Format	Standard Distribution	Final BIAs and physical security assessments provided within 90 days of onsite review
2.2.3.1	BIA Crosswalk Report	Contractor Determined Format	Standard Distribution	Report due August 31
2.2.3.2	ITCP and DRP analyses	Contractor Determined Format	Standard Distribution	Analysis due Mar 1
2.2.3.2	Tabletop COOP exercises	Contractor Determined Format	Standard Distribution	Exercises due Feb 1
2.2.3.2	Functional COOP exercises	Contractor Determined Format	Standard Distribution	Exercises due Mar 1
2.2.3.2	Tabletop COOP after action report	Contractor Determined Format	Standard Distribution	Final report due 30 days after exercise date
2.2.3.2	Functional COOP after action report	Contractor Determined Format	Standard Distribution	Final report due 30 days after exercise date
2.2.4	Security C&A Phase 1 package reviews	Contractor Determined Format	Standard Distribution	Deliverables are provided within agreed upon project plan timeframe

2.2.4	C&A package revisions including required revisions in CSAM	Contractor Determined Format	Standard Distribution	Deliverables are provided within agreed upon project plan timeframe
2.2.4	CSAM Compliance descriptions in CSAM	Contractor Determined Format	Standard Distribution	Deliverables are provided within agreed upon project plan timeframe
2.2.5	Security Metrics Recommendations	Contractor Determined Format	Standard Distribution	Final recommendation developed within 120 calendar DACA
2.2.6	Security Communications Plan	Contractor Determined Format	Standard Distribution	Final Plan developed within 90 calendar DACA
2.2.6	Procedure TRAINING Program	Contractor Determined Format	Standard Distribution	Final Program Plan developed within 180 calendar DACA
2.2.7	Vulnerability Testing and Scanning Report, Server configuration change report	Contractor Determined Format	Standard Distribution	Report delivered by 15th of month
2.2.8	Project plan for Security Program Assessment	Contractor Determined Format	Standard Distribution	Final Plan developed within 60 calendar days of optional task order award
2.2.8	Security Program Improvement plan implementation	Contractor Determined Format	Standard Distribution	Implementation Plan developed within approved project plan timelines
2.2.9	Assessment of FS Centralized Account Management process	Contractor Determined Format	Standard Distribution	Final Plan developed within 60 calendar days of optional task order award
2.2.9	recommendations for account management improvement	Contractor Determined Format	Standard Distribution	Final recommendations due within 120 calendar days of optional task award
2.2.10	Formal evaluation of Technical Approval requests	Contractor Determined Format	Standard Distribution	Evaluation submitted within 20 calendar days after receipt of technical approval request
2.2.11	Process improvement recommendations	Contractor Determined Format	Standard Distribution	Final recommendations due within 180 calendar days of optional task award
2.2.12	Wireless security assessments	Contractor Determined Format	Standard Distribution	Final assessment due within 120 calendar days of optional task award
2.2.13	LAN security assessments	Contractor Determined Format	Standard Distribution	Final assessment due within 120 calendar days of optional task award
2.2.14	Weekly interim status reports	Contractor Determined Format	Standard Distribution	Report due COB Monday
2.2.14	Self Help Documentation	Contractor Determined Format	Standard Distribution	Final documentation due within 60 days of request

5.0 SECTION G: CONTRACT ADMINISTRATION DATA

5.1 CONTRACTING OFFICER'S REPRESENTATIVE

The COR for this order is listed below:

5.2 CONTRACT TYPE FOR THIS ORDER

The Government anticipates that the task order will result in a Firm Fixed Price for labor and Level of Effort for JITR and ODCs on this order.

This is a new requirement.

5.3 PLACE OF PERFORMANCE

5.4 PERIOD OF PERFORMANCE

Period of performance for this order shall be from xxxx

Option 1:
Option 2:

The Contractor shall propose for the base year and 2 option years.

5.5 ANTICIPATED LEVEL OF EFFORT

The Contractor shall provide in its proposal the necessary resources to complete all tasks associated with this effort.

5.6 CONTRACTOR TRAVEL

5.6.1 Travel

Arrangements for and costs of all travel, transportation, meals, lodging, and incidentals are the responsibility of the Contractor. Travel costs shall be incurred and billed in accordance with FAR Part 31. Costs for these expenses will be reviewed and certified by the COR and approved by the Contracting Officer. All travel and transportation shall utilize commercial sources and carriers provided the method used for the appropriate geographical area results in reasonable charges to the government. The Government will not pay for business class or first-class travel. Lodging and meals shall be reimbursed in accordance with the standard per diem rates in the DOD Joint Travel Regulation.

The Contractor shall list the travel required using the following matrix:

From	To	Round Trip (Y/N)	# of Trips	# of People	# of Days

6.0 OTHER TERMS, CONDITIONS, AND PROVISIONS

6.1 INFORMATION ASSURANCE

By accepting this contract/agreement, the Contractor/Cooperator and other external organizations (hereafter called Contractor) providing Information Technology (IT) services to the agency agrees to comply with the applicable IT security policy as outlined in this document. The Contractor and other external organizations will be responsible for

IT security for all systems connected to the FS network or operated by the Contractor and other external organizations for the agency, regardless of location. This clause is applicable to all or any part of the contract that includes IT resources or services in which the Contractor and other external organizations must have physical or electronic access to FS sensitive information that directly support the mission of the Government. The term 'information technology', as used in this clause, means any equipment or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. This includes both major applications and general support systems as defined by OMB Circular A-130.

If new or unanticipated threats or hazards are discovered by either the Government or the Contractor or other external organization, or if existing safeguards have ceased to function, the discoverer will immediately bring the situation to the attention of the other party. The Contractor will report real or suspected incidents or violations to the Computer Incident Response Team (CIRT).

The Contractor shall insert these clauses in all subcontracts when the subcontractor is required to have routine physical access to a Federally-controlled facility and/or routine access to a Federally-controlled information system. Failure to comply with said requirements will constitute cause for termination.

IT Security Training: The Contractor and other external organizations will ensure that its employees performing under this contract fulfill all requirements for mandatory security awareness and role-based advanced security training in accordance with OMB Circular A-130, FISMA, and NIST requirements, and sign all applicable statements of responsibilities.

Background Investigations: All non-government employees with unescorted access to facilities, computer systems and/or information must have background investigations commensurate with the level of risk and magnitude of loss or harm. The Government will determine the level of background investigation and position classification needed.

6.2 PROTECTION OF INFORMATION

6.2.1 FAR 52.224-1 -- Privacy Act Notification (1984)

6.2.2 FAR 52.224-2 -- Privacy Act (1984)

6.2.3 Dissemination of Information/Publishing

The Contractor shall be responsible for properly protecting all information used, gathered, or developed as a result of work under this task. The Contractor shall also protect all unclassified Government data, equipment, etc., by treating information as sensitive business, confidential information, controlling and limiting access to the information, and ensuring the data and equipment are secured within their facility.

To the extent required to carry out a program of inspection to safeguard against threats and hazards to the security, integrity, and confidentiality of Government data, the Contractor will afford the Government access to the Contractor's or other external organization’s facilities, installations, technical capabilities, operations, documentation, records, and databases. The Contractor will cooperate with Federal agencies and their officially credentialed representatives during official inspections or investigations concerning the protection of FS information. Cooperation may include providing relevant documentation showing proof of compliance with federal and agency requirements, and rendering other assistance as deemed necessary.

6.2.4 Identification of Contractor Employees

All contract personnel attending meetings, answering Government telephones, and working in other situations where their contractor status is not obvious to third parties are required to identify themselves as such. They must also ensure that all documents or reports produced by contractors are suitably marked as contractor products or that contractor participation is appropriately disclosed.

6.2.5 Badges

Contractor personnel may be required to attend meetings to meet order requirements. Contractor personnel shall wear Government provided contractor badges in Government spaces during the performance of this order.

6.2.6 Non-Disclosure Agreement

The Contractor shall sign one version of the following Non-disclosure Statement (Appendix B) (Deliverable 1) on behalf of the company, only if applicable, and shall also ensure that all staff assigned to, including all subcontractors and consultants, or performing on this Delivery Order execute and adhere to the terms of the following non-disclosure statement, protecting the procurement sensitive information of the Government and the proprietary information of other contractors. Assignment of staff who have not executed this statement or failure to adhere to this statement shall constitute default on the part of the Contractor.

6.3 PRIVACY ACT

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.

6.4 QUALITY ASSURANCE

The Government will review monthly performance and progress reports and will attend regular task performance review meetings with the Contractor to survey quality of products and services according to the following plan.

6.4.1 Objective

The purpose of this plan is to provide a quality surveillance plan for this delivery order. This plan provides a basis for the COR to evaluate the quality of the Contractor's performance. The oversight provided for in the order and in this plan would help to ensure that service levels reach and maintain the required levels throughout the contract term. Further, this plan provides the COR with a proactive way to avoid unacceptable or deficient performance, and provides verifiable input for the required Past Performance Information Assessments.

6.4.2 Performance Standards Summary Matrix.

See Appendix C.

6.4.2.1 Quality Level

By monitoring the Contractor, the COR will determine whether the performance levels set forth in the order have been attained. Performance standards are specified in the summary matrix.

6.4.2.2 Frequency

During performance of this order, the COR will take periodic measurements, as specified in the Method of Surveillance column of the Summary Matrix, and will analyze whether the negotiated frequency of measurement is appropriate for the work being performed. Adjustments may only be made by a modification to the order.

6.4.3 Surveillance Process

The COR will conduct performance evaluations based on the required standards set forth in the performance standards summary above. The COR will perform random checks of the work products, files, and databases to perform surveillance.

6.4.4 Performance Evaluation Process

The Contractor Performance Assessment Reporting System (CPARS) has been adopted by the agency to electronically capture assessment data and manage the evaluation process. CPARS is used to assesses a contractor's performance and provide a record, both positive and negative, on a given contract during a specific period of time. The CPARS process is designed with a series of checks and balances to facilitate the objective and consistent evaluation of contractor performance. Both government and contractor program management perspectives are captured on the CPAR form and together make a complete CPAR. Once the Assessing Official completes the proposed assessment for the period of performance, the CPARS is released to the appropriate Government Contractor Representative for their review and comments. User ID and Password will be provided to the designated Government Contractor Representative upon issuance of a delivery order. The contractor has 30 days after the Government's evaluation is completed to comment on the evaluation. The Government Contractor Representative must either concur or nonconcur to each CPAR. If the contractor concurs with the proposed assessment and the Reviewing Official does not wish to see the CPAR, the Assessing Official may close out the CPAR. Otherwise, they must forward the CPAR to the Reviewing Official for them to review, enter comments if appropriate, and close out. The Reviewing Official may at their option direct the Assessing Official to forward every CPAR to them for review.

6.5 GOVERNMENT FURNISHED EQUIPMENT (GFE)/ INFORMATION (GFI)/FACILITIES

The Contractor shall maintain an inventory accounting system for Government Furnished Equipment (GFE), Government Furnished Software (GFS), and other Government Furnished Tools. The Contractor shall provide the COR with the information necessary to manage GFE under this PB SOW. All Government Property should be maintained per FAR 52.245-5.

6.5.1 Government Furnished Facilities

If the optional task for vulnerability scanning is exercised, the Government will offer desk space and office furnishings for the Contractor personnel at a Government location.

6.5.2 Government Furnished Equipment/Information

The Contractor shall identify, in their proposal, any Government Furnished Equipment/Information or Contractor-acquired-Government Owned property (CAP), necessary to perform this task. This shall include any Contractor purchased or acquired/ Government-owned items. Detailed Bills of Materials shall be submitted along with the proposal, noting part numbers, prices, and need dates for all required GFE.

The Contractor shall maintain a detailed inventory accounting system for Government Furnished Equipment/Material or CAP. The inventory accounting system must specify, as a minimum: product description (make, model), Government tag number, date of receipt, name of recipient, location of receipt, current location, purchase cost (if CAP), and contract/order number under which the equipment is being used. The Contractor shall either: a) attach an update inventory report to each monthly performance and progress report, or b) certify that the inventory has been updated and is available for Government review. In either case the Contractor's inventory listing must be available for Government review within one business day of COR request.

Upon the request of the Contractor, the Government may provide as GFE the following type of equipment and services to the Contractor's on-site support staff on a case-by-case basis dependent upon individual task and availability:

- PCs with network cards and network access to provide interface with Trouble Ticket System(s) and allow trouble shooting of PC-related emulation customer problems,
- Licensed copies of project required software,
- Utilities such as adequate power, air conditioning, and phones with commercial long distance access speaker capability for conference calls and hands free trouble shooting,

- Access to commercial long distance facsimile,
- Laser printer access, either as individual units with supplies, or an office network printer with LAN card,
- Access to local copiers, supplies, shredder to control the disposal of Privacy Act Materials, and
- Pagers and/or cellular phones if mandated and provided, to include any subscription services, by the local MTF.

6.6 SECTION 508 REQUIREMENT

The Contractor shall comply with Section 508 of the Rehabilitation Act of 1973 (29 U.S.C. 794d). Specifically, the procurement, development, maintenance, or integration of electronic and information technology (EIT) under this contract must comply with the applicable accessibility standards issued by the Architectural and Transportation Barriers Compliance Board at CFR part 1194.

Section 508 Accessibility Standards. The following Section 508 Accessibility Standard(s) (Technical standards and Functional Performance Criteria) are applicable (if box is checked) to this acquisition.

Technical Standards

- ☐ 1194.21 - Software Applications and Operating Systems
- ☒ 1194.22 - Web Based Intranet and Internet Information and Applications
- ☐ 1194.23 - Telecommunications Products
- ☐ 1194.24 - Video and Multimedia Products
- ☐ 1194.25 - Self-Contained, Closed Products
- ☐ 1194.26 - Desktop and Portable Computers
- ☒ 1194.41 - Information, Documentation and Support

The Technical Standards above facilitate the assurance that the maximum technical standards are provided to the Offerors. Functional Performance Criteria is the minimally acceptable standards to ensure Section 508 compliance. This block is checked to ensure that the minimally acceptable electronic and information technology (E&IT) products are proposed.

Functional Performance Criteria

- ☒ 1194.31 - Functional Performance Criteria

7.0 CENTRAL CONTRACTOR REGISTRY

All contractors must be registered in the Central Contactor Registration. This is one of the steps the Federal Government is taking to streamline the acquisition process. In an effort to broaden use and reliance upon e-business applications, the CCR was established to eliminate the need to maintain paper-based sources of contractor information.

8.0 TASK ORDER CLOSEOUT

Task order close out procedures will be issued upon 90 days after this task order has ended. The determination of final costs for this effort shall be requested. This does not preclude the contractor's right to funds invoiced but not

collected, if any. (FAR 42.708) A release of claims document shall be submitted into IT System for action within 90 days of completion of this task by the Contractor.

Close-out of contract files - FAR 4.804.

9.0 CONTRACTOR'S PURCHASING SYSTEMS

The objective of a contractor purchasing system assessment is to evaluate the efficiency and effectiveness with which the contractor spends Government funds and complies with Government policy with subcontracting.

Prior to the award of a task order the Contracting Officer shall verify the validity of the contractor's purchasing system. Thereafter, the contractor is required to certify to the Contracting Officer no later than 30 calendar days prior to the exercise of any options the validity of their purchasing system. Additionally, if reviews are conducted of the purchasing system after the exercise of the option, the contractor shall provide the results of the review to the Contracting Officer within 2 weeks from the date the results are known to the contractor.

10.0 DATA RIGHTS

The Government requires unlimited rights in any material first produced in the performance of this task order, in accordance with the FAR clause at 52.217-14. In addition, for any material first produced in the performance of this task order, the materials may be shared with other agencies or contractors during the period of performance of this task order, or after its termination. For any subcontractors or teaming partners, the Contractor shall ensure at proposal submission that the subcontractors and /or teaming partners are willing to provide the data rights required under this task order.

11.0 FAR CLAUSES

NOTE: Section I of the contractor's Alliant Contract is applicable to this Task Order and is hereby incorporated by reference. In addition, the following applies:

11.1 FEDERAL ACQUISITION REGULATION (48 CFR CHAPTER 1) SOLICITATION CLAUSES (http://www.arnet.gov/far/)

CLAUSE NO	CLAUSE TITLE	DATE
52.204-10	REPORTING EXECUTIVE COMPENSATION AND FIRST-TIER SUBCONTRACT AWARDS	(JUL 2010)
52.215-21 52.215-22	REQUIREMENTS FOR COST OR PRICING DATA OR INFORMATION OTHER THAN COST OR PRICING DATA – MODIFICATIONS	(OCT 1997)
52.216-8	FIXED FEE	(MAR 1997)
52.217-8	OPTION TO EXTEND SERVICES Fill-In Date _Expiration of Task Order Fill-In Date - 30 days Fill-In Date: ____30 days_____	(NOV 1999)
52.217-9	OPTION TO EXTEND THE TERM OF THE CONTRACT	(MAR 2000)
52.219-8	UTILIZATION OF SMALL BUSINESS CONCERNS	(MAY 2004)
52.219-9	SMALL BUSINESS SUBCONTRACTING PLAN	(JUL 2010)
52.223-15	ENERGY EFFICIENCY IN ENERGY CONSUMING PRODUCTS	(DEC 2007)

52.223-16	IEEE 1680 STANDARD FOR THE ENVIRONMENTAL ASSESSMENT OF PERSONAL COMPUTER PRODUCTS	(DEC 2007)
52.227-14	RIGHTS IN DATA – GENERAL ALTERNATE II	(DEC 2007)
52.227-15	REPRESENTATION OF LIMITED RIGHTS DATA AND RESTRICTED COMPUTER SOFTWARE	(DEC 2007)
52.227-16	ADDITIONAL DATA REQUIREMENTS	(JUN 1987)
52.251-1	AUTHORIZATION TO USE GOVERNMENT SUPPLY SOURCES	(AUG 2010)

APPENDIX A

Current Operational Technology Environment

1. The IT component of the Agency's Enterprise Architecture consists of 23,000+ desktop PCs and 22,000+ laptops running Windows XP refreshed on a four- to six-year refresh cycle and supported by over 1,000 Unix®-based (AIX®) and over 200 Linux based X-86 servers, and associated data and voice networks, as well as an extensive radio infrastructure comprised of tens of thousands of portable (handheld) and mobile radios and associated base stations, repeaters, and other equipment. Desktop and laptop computers connect to the Agency's Distributed Computing Environment/Distributed File System (DCE/DFS) environment through a server operating system component named Fast Connect for AIX, which enables Microsoft® Windows® clients to access AIX file systems and printers using the Server Message Block (SMB) networking protocol. See Exhibit #1 for Representative Infrastructure Devices and Services.

2. The Agency is migrating from the Unix®-based (AIX®) Mid-Range servers, located in over 150 locations, to an architecture based on X-86 server and Linux located in two data centers. The Agency also has deployed significant numbers of handheld computers including, but not limited to, Windows CE® (Pocket PC), Palm®-based systems, and Blackberry OS in both office and field/outdoor ruggedized configurations, and uses both wireless (e.g., radio, satellite) and wired facilities to support remote sensing and telemetry applications. The FS has 200 regional applications to migrate to the data center.

3. The Government has implemented several components of the Tivoli® Enterprise Management system for providing Enterprise-wide operational monitoring capability (server and desktop monitoring, control, and troubleshooting facilities). Components include Tivoli Service Desk, Tivoli Framework, Tivoli Management Region, Tivoli Trusted Information Systems, Tivoli Remote Control, and Tivoli Endpoints. Additionally, the Forest Service has deployed Computer Associates' UAPM for Asset Management.

4. COTS software packages are installed as part of the standard image and include ERDAS® Remote Sensing Software, ESRI® Geographic Information Systems software, Lotus Notes®/Domino® mail and collaboration software, Microsoft Office® Software, Oracle® software, Web browsers, and may include other software depending on requirements.

5. The agency has over 7,000 networked output devices (printers, plotters, and digitizers) located across the Agency. Over 6,000 of these devices are laser printers connected to the network. The Agency deploys its networked output devices only after performing extensive testing (conducted by the ISO) in its integration lab.

6. To comply with the requirements of the Americans with Disabilities Act (also known as Section 508), the Agency procures a variety of software and hardware devices ("adaptive aids"). The hardware devices include Braille printers, speech synthesizers, video magnifiers, and other equipment.

7. The Chief Information Office (CIO) supports 42,000 users across 40 major systems. The FS security policy document resides in the Agency policy manual system under the 6680 section. This 6680 section is divided into two parts consisting of approximately 240 pages. There are roughly 90 IT security procedures that ensure compliance with FISMA direction.

8. The agency has directed all of its agencies to convert to Exchange Email (Outlook) by October, 2010. Active Directory is also implemented across the Forest Service.

9. Throughout the solicitation the agency has described its future plans in the most accurate fashion possible based on the currently available plans. Future IT planning may change; the agency will endeavor to be transparent and timely in its communication of planning changes.

10. Representative Operation Center services and FS Infrastructure Devices are listed below.

Current Contact Center Environment

Today's Customer Help Desk is operated and managed by XXX in a Contract that was awarded in XXXX. In today's environment, calls and web-entered tickets are the principal form of communication with the helpdesk; also web-chat is provided in today's environment.

Representative Desktop, Laptop, and High-End Workstation Hardware

1. <u>Desktop</u>

    a) Dell Optiplex GX, Precision, Dimension
    b) IBM 6578, 6792, 6794, 6862, 6892, 6833, 6840
    c) Lenovo Think Centre

2. <u>Laptop</u>

    a) Dell D400, D600, D800, M50, M60, X300
    b) IBM 2530, 2626, 2828, 2652, 2662
    c) Lenovo ThinkPad T60, X60

3. High-End Workstation

    a) IBM 7043-240

Representative Servers

1. Dell Power Edge

    a) Model 1650, 1750, 2600, 2650, 2850, 6650

2. IBM RS/6000 7019, 7013, 7015, 7030

    a) Model C20, 590, 620, J40, R40, 9076

3. IBM eServer xSeries

    a) Model 330, 345, 346,

4. IBM Server

    a) 7028, 7029, 7038, 7043, 7044, 7046, 9111, 9113, 9117

5. IBM PPS (Personal Power System)

Representative Network Printers and Multi-function Devices

1. Hewlett Packard Color Laser Jet

    a) Model 3XXX, 4XXX, 5XXX

2. Hewlett Packard Design Jet

    a) Model 1055cm, 5XXX, 6XX, 7XX

3. Hewlett Packard Laser Jet

    a) Model 2XXX, 3XXX, 4XXX, 5XXX, 8XXX

4. Lexmark Optra

    a) Series C, S, T ,W

5. Xerox Phaser

    a) Model 3XXX, 4XXX, 5XXX, 6XXX, 7XXX

6. Xerox

    a) WorkCenter Pro 45, WorkCenter Pro 65
    b) Document Centre 432ST

Representative Blackberry and PDA Devices

1. Approximately 2000 users (as of Dec 2009) with:

    a) Dell Axim X51; and
    b) Blackberry 7130e, 8700, 8830, 9830

Network Operations Center (NOC)

1. The Network Operations function is comprised of two Network Operations Centers for redundancy – one in Albuquerque, NM and one in Portland, OR. Each NOC has monitors that display continuous Big Brother and Concord e-Health status. The Forest Service uses MRTG (Multi Router Traffic Grapher) to check specific connections when troubleshooting problems. The NOC also utilizes CNN to watch for adverse weather conditions or events. Additional tools in use today include Spectrum and Cisco Works 2000. Future tools may vary as requirements dictate.

Security Operations Center (SOC)

1. The Security Operations Group is responsible for two distinctly different, yet complimentary, functions: security operations and computer incident response. The Forest Service Computer Incident Response Team (CIRT) responds to security incidents that are originated from several sources including the OCIO, US-CERT, complaints from the public and from the Security Group's analysis of information collected through the security operations aspect of the group. The CIRT is responsible for following computer incidents from their inception through successful incident resolution. This includes following Federal and agency guidelines for incident reporting, coordinating different lines of service (LOS) groups within the Forest Service and forensic analysis of both network packet captures and full computer systems. The CIRT must be available 24x7 to respond to any security incident as it arises.

2. The security operations area is the primary monitor of the Forest Service's network security state. Currently this is accomplished using a variety of tools including Cisco Intrusion Detection System, NetForensics, ISS Internet Scanner and Symantec Endpoint Protection, although these tools are constantly being reviewed against current industry offerings to provide the best security cost/benefit for the Forest Service. These tools are currently monitored from geographically disparate locations in a 10x5 mode of operation. The Security Group is in the process of migrating this functionality to a 24x7 capacity for more comprehensive coverage of the security posture.

3. The Security Group is also responsible for the interface between the Forest Service and the Forest Service's Internet Service Provider (ISP) for security. This includes development of firewall rules for the Forest

Service's ISP using Cisco technology and CIRT integration for responding to security incidents the ISP may pick up.

Enterprise Operations Center (EOC)

The Enterprise Operations Center:

1. Monitors the IT infrastructure including network, services, critical services, business applications, radio and telephone components;
2. Tracks performance against service levels;
3. Provides 24x7 support through the combined resources of the EOC and Duty officer Process; and
4. Provides services including Incident Management, Problem Management, Change Management, Availability Management, and Release Management.

Appendix B: Performance Based Matrix						
CRIS PERFORMANCE REQUIREMENTS SUMMARY						
REQUIRED SERVICE	TASK ORDER NUMBER	DESCRIPTION	STANDARD	ACCEPTABLE QUALITY LEVEL	METHOD OF SURVEILLANCE	INCENTIVE OR DISINCENTIVE
Task Management	2.1	Provide final Project Plan	Project Plan submitted no later than 1 month from award and changes in draft Project Plan as required by Government.	99% quality as presented in task order award and on time	100% Inspection	Invoice deduction of $1000 for not meeting AQL or delivery date
Task Management	2.1	Prepare and update, as needed, Program Management Plan and Quality Assurance Plan	Plans developed, reviewed and updated within 15 calendar DACA	95% quality as presented in task order award and on time	100% Inspection	Invoice deduction of $1000 for not meeting AQL or delivery date. Rework will be allowed.
Task Management	2.1	Prepare Monthly Performance and Progress Reports and participate in status conference calls	Prepare within 10 business days after month end and 99% participation in status calls.	100% quality as presented in task order award and on time	100% Inspection	Invoice deduction of $1000 for not meeting AQL or delivery date.
Security Documentation Management	2.2.1	Evaluate and recommend a security documentation management solution and submit a plan for implementation	Recommendation and plan submitted within 120 DACA	100% quality as presented in task order award and on time	100% Inspection	Invoice deduction of $5,000 for not meeting AQL or delivery date. Rework will be allowed.
Security Documentation Management	2.2.1	Implementation of a security documentation management solution	Implementation completed within 45 days of accepted security documentation management plan	100% quality as presented in task order award and on time	100% Inspection	Invoice deduction of $1000 for not meeting AQL or delivery date.
Security Documentation Management	2.2.1	Provide Gap Analysis on FS IT Security Policy and Procedures against USDA policy and procedures	Report provided by January 15	100% quality as presented in task order award and on time	100% Inspection	Invoice deduction of $1000 for not meeting AQL or delivery date. Rework will be allowed.

REQUIRED SERVICE	TASK ORDER NUMBER	DESCRIPTION	STANDARD	ACCEPTABLE QUALITY LEVEL	METHOD OF SURVEILLANCE	INCENTIVE OR DISINCENTIVE
Security Documentation Management	2.2.1	Provide Report on Security Policy and Procedure Effectiveness	Report provided by August 1	100% quality as presented in task order award and on time	100% Inspection	Invoice deduction of $1000 for not meeting AQL or delivery date. Rework will be allowed.
Security Documentation Management	2.2.2.1	Annual Security Policy Currency review	Policy review submitted by November 1	100% quality as presented in task order award and on time	100% Inspection	Invoice deduction of $5,000 for not meeting AQL or delivery date. Rework will be allowed.
Security Documentation Management	2.2.2.1	Annual Security Procedure Currency review	Reviews submitted within 11 months of government's last approval date	98% quality as presented in task order award and on time	100% Inspection	Invoice deduction of $1000 for not meeting AQL or delivery date. Rework will be allowed.
Regulatory Analysis	2.2.2.2	Analyze new federal government requirements and develop tailored recommendation developed, reviewed and updated	Recommendation developed, reviewed and updated within 60 days of date of issuance of new federal regulations or requirements	95% quality as presented in task order award and on time	100% Inspection	Invoice deduction of $1000 for not meeting AQL or delivery date. Rework will be allowed.
Risk Management Framework and Strategy	2.2.1.3	Develop Risk Management Framework Strategy and Concept of Operations (ConOps)	Final Strategy developed with 60 days of task order award and ConOps developed within 60 days of approved strategy	95% quality as presented in task order award and on time	100% Inspection	Invoice deduction of $1000 for not meeting AQL or delivery date. Rework will be allowed.
Risk Management Framework and Strategy	2.2.1.3	Provide Risk Management Framework Implementation plan	Plan developed, reviewed and updated within 60 days of ConOps approval	95% quality as presented in task order award and on time	100% Inspection	Invoice deduction of $1000 for not meeting AQL or delivery date. Rework will be allowed.

REQUIRED SERVICE	TASK ORDER NUMBER	DESCRIPTION	STANDARD	ACCEPTABLE QUALITY LEVEL	METHOD OF SURVEILLANCE	INCENTIVE OR DISINCENTIVE
Risk Management Framework and Strategy	2.2.1.3	Provide annual update to Risk Management Framework	Updated Framework provided by September 30	95% quality as presented in task order award and on time	100% Inspection	Invoice deduction of $1000 for not meeting AQL or delivery date. Rework will be allowed.
Security Program Plan	2.2.1.4	Develop Information Security Program Plan	Final Program Plan developed within 120 days of task order award	95% quality as presented in task order award and on time	100% Inspection	Invoice deduction of $1000 for not meeting AQL or delivery date. Rework will be allowed.
Security Program Plan	2.2.1.4	Provide annual update of Information Security Program Plan	Updated Security Plan provided by July 30	95% quality as presented in task order award and on time	100% Inspection	Invoice deduction of $1000 for not meeting AQL or delivery date. Rework will be allowed.
A-123 Assessment and Continuous Monitoring	2.2.2.1	Develop and execute project plans for A-123 internal control assessments, reporting results, providing recommendations and entering results in CSAM	Plans, assessments, and reports developed, reviewed, completed and reported in CSAM by May 1	99% quality as presented in task order award and on time	Random sampling	Invoice deduction of $1000 for not meeting AQL or delivery date. Rework will be allowed.
A-123 Assessment and Continuous Monitoring	2.2.2.1	Develop plans for corrective actions of all non-compliant security controls	Recommendation developed by June 15	99% quality as presented in task order award and on time	Random sampling	Invoice deduction of $1000 for not meeting AQL or delivery date. Rework will be allowed.
A-123 Assessment and Continuous Monitoring	2.2.2.1	Design, develop and implement a continuous monitoring process	Plan developed, reviewed and implemented within 180 days of task order award	95% quality as presented in task order award and on time	100% Inspection	Invoice deduction of $1000 for not meeting AQL or delivery date. Rework will be allowed.

REQUIRED SERVICE	TASK ORDER NUMBER	DESCRIPTION	STANDARD	ACCEPTABLE QUALITY LEVEL	METHOD OF SURVEILLANCE	INCENTIVE OR DISINCENTIVE
IT Security Support to Data Center Application Migration	2.2.2.2	Perform system categorizations on applications/tables migrating to Data Centers and report results to management	Categorizations and results developed within 90 days after task order award for every lot of 25 migrations, status reports due NLT 10th of month	99% quality as presented in task order award and on time	100% Inspection	Invoice deduction of $1000 for not meeting AQL or delivery date. Rework will be allowed.
Contingency Plan Development and Evaluation	2.2.3.1	Develop and revise POW for BIAs, Business Impact Analyses, physical security assessments and crosswalk report	POW due Nov 1, Final BIAs and physical security assessments provided within 90 days of onsite review, report due Sept 1	95% quality as presented in task order award and on time	Random sampling	Invoice deduction of $1000 for not meeting AQL or delivery date. Rework will be allowed.
Contingency Plan Development and Evaluation	2.2.3.1	Review and analyze IT Contingency Plans and Disaster Recovery Plans, and assist with updating IT Continuity of Operation Plans, Crisis Management Plan, Communication and other contingency documents	Annual reviews provided by March 1	95% quality as presented in task order award and on time	Random sampling	Invoice deduction of $1000 for not meeting AQL or delivery date. Rework will be allowed.
Contingency Plan Exercise and Training	2.2.3.2	Design, conduct and document system level ITCP and DRP notification drills and table top exercises for up to 40 IT systems, and COOP exercises for several national headquarter locations and at enterprise IT leadership level	Tabletop exercises due Feb 1, Functional exercises due Mar 1, Final reports delivered 30 days after exercise date	95% quality as presented in task order award and on time	Random sampling	Invoice deduction of $1000 for not meeting AQL or delivery date. Rework will be allowed.

REQUIRED SERVICE	TASK ORDER NUMBER	DESCRIPTION	STANDARD	ACCEPTABLE QUALITY LEVEL	METHOD OF SURVEILLANCE	INCENTIVE OR DISINCENTIVE
Certification and Accreditation Coordination	2.2.4	Conduct reviews of documentation to prepare or revise C&A packages for a General Support System and loaded into CSAM	Deliverables are provided on time within agreed upon project plan timeframe	90% of deliverables on time, balance due within 1 week; 95% quality as presented in task order award and on time	Random sampling	Invoice deduction of 5% for not meeting AQL or delivery date. Rework will be allowed.
Certification and Accreditation Coordination	2.2.4	Conduct reviews of documentation to prepare or revise C&A packages for a major application and loaded into CSAM	Deliverables are provided on time within agreed upon project plan timeframe	90% of deliverables on time, balance due within 1 week; 95% quality as presented in task order award and on time	Random sampling	Invoice deduction of 5% for not meeting AQL or delivery date. Rework will be allowed.
Security Metric reporting	2.2.5	Develop plan to collect and present Security Metrics	Plan developed, reviewed and implemented within 120 calendar DACA	95% quality as presented in task order award and on time	100% Inspection	Invoice deduction of $1000 for not meeting AQL or delivery date. Rework will be allowed.
Security Metric reporting	2.2.5	Implement the Security Metrics Plan	Implementation completed within approved Security Metrics plan timeframe	95% quality as presented in task order award and on time	100% Inspection	Invoice deduction of $1000 for not meeting AQL or delivery date. Rework will be allowed.
Information Security Outreach and Awareness	2.2.6	Develop a comprehensive Security Communications Plan	Plan developed within 90 calendar DACA	95% quality as presented in task order award and on time	100% Inspection	Invoice deduction of $1000 for not meeting AQL or delivery date. Rework will be allowed.
Information Security Outreach and Awareness	2.2.6	Implement the Security Communications Plan	Implementation completed within approved Security Communication plan timeframe	95% quality as presented in task order award and on time	100% Inspection	Invoice deduction of $1000 for not meeting AQL or delivery date. Rework will be allowed.

REQUIRED SERVICE	TASK ORDER NUMBER	DESCRIPTION	STANDARD	ACCEPTABLE QUALITY LEVEL	METHOD OF SURVEILLANCE	INCENTIVE OR DISINCENTIVE
Information Security Outreach and Awareness	2.2.6	Develop a Security Procedure Training Plan	Final Plan developed within 180 calendar DACA	95% quality as presented in task order award and on time	100% Inspection	Invoice deduction of $1000 for not meeting AQL or delivery date. Rework will be allowed.
Vulnerability Scanning and Auditing	2.2.7	Provide report on scanning results	Report delivered by the 15th of month	99% quality as presented in task order award and on time	100% Inspection	Invoice deduction of $1000 for not meeting AQL or delivery date. Rework will be allowed.
Vulnerability Scanning and Auditing	2.2.7	Provide report on Server configuration change results	Report delivered by the 15th of month	99% quality as presented in task order award and on time	100% Inspection	Invoice deduction of $1000 for not meeting AQL or delivery date. Rework will be allowed.
Security Program Support	2.2.8	Develop plan for assessing the performance of the FS Security Program	Plan developed, reviewed and updated within 2 months of optional task award	95% quality as presented in task order award and on time	100% Inspection	Invoice deduction of $1000 for not meeting AQL or delivery date. Rework will be allowed.
Security Program Support	2.2.8	Implement the plan the FS Security Program assessment	Implementation completed within approved Security Program Assessment plan timeframe	95% quality as presented in task order award and on time	100% Inspection	Invoice deduction of $1000 for not meeting AQL or delivery date. Rework will be allowed.
Centralized Account Management Support	2.2.9	Provide assessment of FS centralized account management.	Assessment developed, reviewed and updated within 2 months of optional task award	95% quality as presented in task order award and on time	100% Inspection	Invoice deduction of $1000 for not meeting AQL or delivery date. Rework will be allowed.

REQUIRED SERVICE	TASK ORDER NUMBER	DESCRIPTION	STANDARD	ACCEPTABLE QUALITY LEVEL	METHOD OF SURVEILLANCE	INCENTIVE OR DISINCENTIVE
Centralized Account Management Support	2.2.9	Provide plan for centralized account management improvement	Plan developed, reviewed and updated within 120 calendar days after optional task award	95% quality as presented in task order award and on time	100% Inspection	Invoice deduction of $1000 for not meeting AQL or delivery date. Rework will be allowed.
Technical Approval Support	2.2.10	Provide formal evaluation recommendations for technical approval requests	Recommendation submitted within 20 days after optional task award	95% quality as presented in task order award and on time	100% Inspection	Invoice deduction of $1000 for not meeting AQL or delivery date. Rework will be allowed.
IT Security Process Improvement	2.2.11	Provide recommendations for IT Security Process Improvement	Recommendation developed, reviewed and updated within 6 months of optional task award	95% quality as presented in task order award and on time	100% Inspection	Invoice deduction of $1000 for not meeting AQL or delivery date. Rework will be allowed.
Wireless Assessment	2.2.12	Provide assessment of FS wireless network	Final assessment due within 120 calendar days of optional task award	95% quality as presented in task order award and on time	100% Inspection	Invoice deduction of $1000 for not meeting AQL or delivery date. Rework will be allowed.
Network Assessment	2.2.13	Provide assessment of FS local area networks	Final assessment due within 120 calendar days of optional task award	95% quality as presented in task order award and on time	100% Inspection	Invoice deduction of $1000 for not meeting AQL or delivery date. Rework will be allowed.
Program Support	2.2.14	Weekly Status Reports	Report due COB Monday	95% quality as presented in task order award and on time	100% Inspection	Invoice deduction of $1000 for not meeting AQL or delivery date. Rework will be allowed.

REQUIRED SERVICE	TASK ORDER NUMBER	DESCRIPTION	STANDARD	ACCEPTABLE QUALITY LEVEL	METHOD OF SURVEILLANCE	INCENTIVE OR DISINCENTIVE
Program Support	2.2.14	Self Help documentation	Final documentation due 60 days after government request	95% quality as presented in task order award and on time	100% Inspection	Invoice deduction of $1000 for not meeting AQL or delivery date. Rework will be allowed.