ORDER FOR SUPPLIES OR SERVICES

PAGE 1 OF PAGES 1

IMPORTANT: Mark all packages and papers with contract and/or order numbers. BPA NO. DR-33-05-386

1. DATE OF ORDER 11/04/05
2. CONTRACT NO. (If any) GS35F0229K
3. ORDER NO. DR-33-05-386-T004 MODIFICATION NO.
4. REQUISITION/REFERENCE NO. CIO-05-386-004
5. ISSUING OFFICE (Address correspondence to)
U.S. Nuclear Regulatory Commission
Div. of Contracts
Attn:
Mail Stop T-7-I-2
Washington, DC 20555

6. SHIP TO:
a. NAME OF CONSIGNEE
U.S. Nuclear Regulatory Commission
ATTN: CARL KONZMAN
b. STREET ADDRESS
Mail Stop: T-6F41
c. CITY Washington
d. STATE DC
e. ZIP CODE 20555
f. SHIP VIA

7. TO:
a. NAME OF CONTRACTOR
MAR, INCORPORATED
b. COMPANY NAME
c. STREET ADDRESS
1803 RES BLVD STE 204
d. CITY ROCKVILLE
e. STATE MD
f. ZIP CODE 208506106

8. TYPE OF ORDER
[ ] a. PURCHASE
Reference your _____
Please furnish the following on the terms and conditions specified on both sides of this order and on the attached sheet, if any, including delivery as indicated.
[X] b. DELIVERY
Except for billing instructions on the reverse, this delivery/task order is subject to instructions contained on this side only of this form and is issued subject to the terms and conditions of the above-numbered contract.

9. ACCOUNTING AND APPROPRIATION DATA
TRANSFER THE FOLLOWING FUNDS FROM BASIC AWARD AND MOD ONE OF DR-33-05-386 TO TASK ORDER DR-33-05-386-T004: $140,940.10
B&R 510-15-5H2-357 JC: N7235 BOC:252A FS:31X0200

10. REQUISITIONING OFFICE CIO
OIS/BPIAD/ADMB

11. BUSINESS CLASSIFICATION (Check appropriate box(es))
[X] a. SMALL
[ ] b. OTHER THAN SMALL
[ ] c. DISADVANTAGED
[ ] g. SERVICE-DISABLED VETERAN-OWNED
[ ] d. WOMEN-OWNED
[ ] e. HUBZone
[ ] f. EMERGING SMALL BUSINESS

12. F.O.B. POINT
Destination

13. PLACE OF
a. INSPECTION Rockville, MD
b. ACCEPTANCE Rockville, MD

14. GOVERNMENT B/L NO.

15. DELIVER TO F.O.B. POINT ON OR BEFORE (Date)

16. DISCOUNT TERMS
Net 30

17. SCHEDULE (See reverse for Rejections) See CONTINUATION Page

ITEM NO. (A)	SUPPLIES OR SERVICES (B)	QUANTITY ORDERED (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)	QUANTITY ACCEPTED (G)
	The Contractor shall provide the U.S. Nuclear Regulatory Commission with "Major Systems Certification & Accreditation - (HRMS)" in accordance with the attached Performance Based Statement of Work, the terms and conditons of GSA Contract GS-35F-0229K and the attached schedule. ATTACHMENTS: 1. Schedule 2. Statement of Work ACCEPTANCE: [signature] 11/19/2005 SIGNATURE DATE Michael P. Norcio Chairman and CEO PRINT NAME/TITLE	[redacted]			$140,940.10	

18. SHIPPING POINT
19. GROSS SHIPPING WEIGHT
20. INVOICE NO.

21. MAIL INVOICE TO:
a. NAME
U.S. Nuclear Regulatory Commission
Payment Team, Mail Stop T-7-I-2
b. STREET ADDRESS (or P.O. Box)
Attn: Valerie Whipple DR-33-05-386-T004
c. CITY Washington
d. STATE DC
e. ZIP CODE 20555

SEE BILLING INSTRUCTIONS ON REVERSE

17(h) TOTAL (Cont. pages)

17(i). GRAND TOTAL 140,940.10

22. UNITED STATES OF AMERICA BY (Signature) [signature]

23. NAME (Typed)
Valerie M. Whipple
Contracting Officer
TITLE: CONTRACTING/ORDERING OFFICER

AUTHORIZED FOR LOCAL REPRODUCTION
PREVIOUS EDITION NOT USABLE

OPTIONAL FORM 347 (REV. 3/2005)
PRESCRIBED BY GSA/FAR 48 CFR 53.213(e)

TEMPLATE - ADM001

SISP REVIEW COMPLETE

ADM002

PERFORMANCE BASED STATEMENT OF WORK
Task Order #4

PROJECT TITLE: Major Systems Certification and Accreditation -HRMS

TECHNICAL MONITOR: John Bird

PROJECT MANAGER: Carl Konzman
ALTERNATE PROJECT OFFICER: Harry Kromer

1.0 Background

The purpose of this task order is to obtain contractor professional services to assist the NRC in its information technology's security certification and accreditation process implementation. The contractor will assist NRC system owners with the development of security related documentation and systems analysis services required to obtain an authority to operate (i.e., operate the system in compliance with required standards) by providing a centralized security support services that will ensure cradle to grave compliance with FISMA, FEA, OMB M-04-04, NIST 800 Series, other applicable OMB and NIST series security certification and accreditation requirements.

2.0 Objective

The Contractor shall support the OIS in certification and accreditation of the Human Resources Management System (HRMS). HRMS is considered a "Major", high security control baseline information system such that NRC is in compliance and maintains certification and accreditation currency with NIST and FISMA Guidance. The contractor shall at a minimum develop associated certification and accreditation documentation consistent with the security support task referenced in the PBSOW such that an authority to operate (ATO) which confers full accreditation shall be granted the system. The contractor shall perform these security support tasks specified for LOW, MODERATE, and HIGH security baseline systems for each system category "Major", "General Support System", "Listed", and "Other."

To assist NRC in this task the contractor shall develop at a minimum the following information system security certification documentation: a security categorization, a risk assessment, a systems security plan, a security test and evaluation plan and associated report, a contingency test plan and report, and a plan of action and milestones to correct any identified deficiencies.

3.0 Level of Effort

The estimated level of effort for this task is 2 FTE.

4.0 Period of Performance

The period of performance of this task order will start on August 29, 2005 and expire on March 31, 2006.

5.0 Scope of Work

The contractor shall provide security analyst staff and develop all requisite systems certification and accreditation documentation such that all systems obtain an Authority to Operate (ATO) and no system crosses fiscal year boundaries with an Interim Authority to Operate (IATO).

Contractor shall provide a security analyst staff and the development of the documentation associated with the security support tasks specified below for LOW, MODERATE, and HIGH Baseline systems for the system category "Major".

The term "Major Application" means a computerized information system or application that requires special attention to security because of the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. Because of their impact on the agency mission and the information they contain or process, MA's require special management oversight. (See OMB Circular A-130, Appendix III.) For example, an agency wide financial management system containing NRC's official financial records would be a MA. A computer program or a spreadsheet designed to track expenditures against an office budget would not be considered an MA. Similarly, commercial off-the-shelf software products (such as word processing software, electronic mail software, utility software, or general purpose software) would not typically be considered MA's.

To assist NRC in this task the contractor will:

Subtask 1:

Develop and implement a project plan to ensure completion of all certification and accreditation task within the period of performance.

Subtask 2:

Security Categorization

The contractor shall conduct a facilitated security scoping interview to determine the proper system or applications classification and impact consistent with NRC Management Directive 12.5, OMB Circular A-130, Federal Information Processing Standards (FIPS) Publication 199, and NIST Special Publication Series 800. Systems shall be categorized as Major, General Support System, Listed, or Other with a system impact of low, moderate, or high.

The contractor shall develop a systems security scoping report that identifies the system investment, system scope, inter-systems connectivity (diagram intersystem connections, data architecture, mapping, and data element definition and exchange between systems), the information sensitivity levels of data processed within the system, the privacy impact of the system and whether it contains information in identifiable form (IFF), the electronic transactions (Inquire, Create, Delete, and Modify) and requisite authentication level, and electronic records disposition.

Privacy Impact Assessment

The contractor shall complete privacy impact assessments consistent with Section 208 of the Electronic Government Act as part of the security scoping report.

Electronic Records Management Disposition

The contractor shall conduct an electronic records management interview and complete an NRC Form 616 for all NRC IT systems consistent with Code of Federal Regulations Part 36 and OMB Circular A-130 as part of the security scoping report.

E-Authentication Risk Assessments

Under Task Order No. 1 entitled "E-Authentication" to this delivery order, the contractor shall conduct the E-Authentication risk assessments and generate an E-Authentication risk assessment report consistent with

OMB M04-04 and NIST Special Publication 800-30. The E-Authentication risk assessments and E-Authentication risk assessment report shall be incorporated into the security scoping report. Work completed under Task Order No. 1. to this delivery order shall not be billed under this task.

Subtask 3:

Security Control Assessment (SCA)

A full 800-53A security control testing, referred to as a Security Control Assessment (SCA), shall be included I the ST&E Plan/Report. The Contractor shall estimate the development of the SCA test plan and 1 execution and report of the SCA test plan. The SCA test plan will be the basis for a full ST&E plan that shall include both the full security control testing and the full functional or application specific functional security controls. The SCA shall be tailored to the ST&E deliverable in the ST&E Test report in Subtask 8.

Subtask 4:

Contingency Plan

The contingency plan shall be developed in accordance with NIST SP 800-34 "Contingency Planning Guide for Information Technology Systems," NIST SP 800-37 "Guide for the Security Certification and Accreditation of Federal Information Systems," and the NRC Contingency Plan (CP) Template. The contractor shall provide detailed procedures for the notification and activation phase, recovery operations, and return to normal operations. The procedures shall contain sufficient detail that a technically trained individual not familiar with the system can successfully follow the procedures. The system contingency plan shall also contain sufficient personnel contact information to enable contact at all times, vendor contact information to enable contact at all times, equipment (hardware and software) and specification information to enable reconstitution of the system from scratch, all service level agreements and memoranda of understanding, the IT standard operating procedures for the system, identification of any systems that this system is dependent upon along with references for the applicable contingency plans, references to the emergency management plan and occupant evacuation plan, and references to the appropriate continuity of operations plan.

The system contingency plan shall be documented in a report that follows the NRC Template for System Contingency Plan. The report shall be delivered in draft form and then in pre-Test form after NRC comments are incorporated. The NRC IT Security staff review of the draft is required to ensure compliance. The contractor shall update the system contingency plan after completion of the contingency plan test report to reflect validated information. The NRC Senior IT Security Officer must approve the final report to enable system accreditation.

Subtask 5:

Full Contingency Planning Test and Report

The contractor shall provide expert advice and support during the Contingency Planning Test to ensure test plan documentation is compliant with the System Contingency Plan (CP) that has been approved by the NRC Senior Information Technology Security Officer (SITSO). Testing shall follow the test procedures documented in the CP. The contractor shall document the testing in a System Contingency Test Report (CP Test Report). The CP Test Report shall be developed in accordance with NIST SP 800-34 "Contingency Planning Guide for Information Technology Systems," NIST SP 800-37 "Guide for the Security Certification and Accreditation of Federal Information Systems," and the NRC Contingency Test Report Template.

The CP Test shall be documented in a report that follows the NRC Template for NRC Contingency Test Report. The CP Test Report shall identify all testing assumptions, constraints, and dependencies as well

as any anomalies, impromptu tests, and deviations encountered during testing. The CP Test Report shall include the actual testing schedule and detailed test results for each test procedure outlining specific errors encountered. The CP Test Report shall include a table of test findings incorporating any test issues and recommendations. The CP Test Report shall identify any problems encountered during testing and identify the resulting action items for the system. The CP Test Report shall be delivered in draft form and then in final form after NRC comments are incorporated. The NRC Senior Information Technology Security Officer (SITSO) must approve the final CP Test Report to enable system accreditation.

Subtask 6:

Risk Assessment.

The assessment of risk and the development of system security plans are two important activities in an agency's information security program that directly support security accreditation and are required by the Federal Information System Management Act (FISMA) and OMB Circular A-130, Appendix III. Risk assessments influence the development of the security controls for information systems and generate much of the information needed for the associated system security plans.

The risk assessment shall characterize the information processed by using Federal Information Processing Standard (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories. The risk assessment shall follow NIST SP 800-37 "Guide for the Security Certification and Accreditation of Federal Information Systems," and include the following:

- Identification of user types and associated roles and responsibilities
- Identification of risk assessment team members and their associations
- A description of the risk assessment approach and techniques, where the techniques include documentation review, interviews, observation, and hands-on system assessment
- A description of the risk scale used, including at a minimum, the potential impact as defined in FIPS 199, and likelihood as defined in NIST SP 800-30, Risk Management Guide for Information Technology Systems
- A list of potential system vulnerabilities
- A list of potential threat-sources applicable to the system, including natural, human, and environmental threat-sources
- A table of vulnerability and threat-source pairs and observations about each
- Detailed findings for each vulnerability and threat-source pair discussing the possible outcome if the pair is exploited; existing controls to mitigate the pair; the likelihood determination as high, moderate, or low; the impact determination expressed as high, moderate, or low; the overall risk rating based upon the risk scale; and the recommended controls to mitigate the risk
- A summary that includes the number of high, moderate, and low findings and provides a list of prioritized action items based upon the findings.

The risk assessment shall be documented in a report that follows the NRC Template for Risk Assessment Report. The report shall be delivered in draft form and then in final form after NRC comments are incorporated. The NRC IT Security staff review of the draft is required to ensure compliance. The NRC Senior IT Security Officer must approve the final report to enable system accreditation.

The contractor shall track any residual risk in the plan of action and milestones (POA&M). The contractor shall document the results of the process. This shall include documenting the risk number, a description of each risk, the type of risk (i.e., impacting the confidentiality, integrity, or availability), the level of risk (i.e., low, moderate, or high), the associated controls, and the action(s) required or actually performed to eliminate or minimize each risk. The goal is for NRC and contractor personnel to remediate all high and

moderate security findings, and track the remaining security findings in the POA&M.

Subtask 7:

Systems Security Plan (SSP)

The security plan shall be developed in accordance with NIST SP 800-53 and 800-53A "Recommended Security Controls for Federal Information Systems," NIST SP 800-37 "Guide for the Security Certification and Accreditation of Federal Information Systems," and the NRC IT Security Plan Template. The contractor shall identify within the SSP the necessary security controls required, citing the security controls that are in place, those that are planned, and those that are not applicable.

Where a system relies upon a control that is provided by another system (e.g. the NRC LAN/WAN), the specific control being relied upon shall be noted along with the name of the system providing that control. The contractor shall trace the security controls to specific documented guidance, NRC policy (e.g., Management Directives), infrastructure policy or procedures.

The system security plan shall be documented in a report that follows the NRC Template for System Security Plan. The report shall be delivered in draft form and then in pre-System Security Test and Evaluation (ST&E) form after NRC comments are incorporated. The NRC IT Security staff review of the draft is required to ensure compliance. The contractor shall update the system security plan after completion of the ST&E test report to reflect validated in-place and planned controls. The NRC Senior IT Security Officer must approve the final report to enable system accreditation.

Subtask 8:

Full System Test and Evaluation (ST&E) Plan

The contractor shall develop a full System Security Test and Evaluation Plan (STE Plan). The system STE Plan shall be developed in accordance with NIST SP 800-53 and 800-53A "Recommended Security Controls for Federal Information Systems," NIST SP 800-37 "Guide for the Security Certification and Accreditation of Federal Information Systems," and the NRC System Security Test and Evaluation Plan Template. The contractor shall provide detailed test procedures to ensure all IT security functional and assurance requirements are fully tested. The procedures shall contain sufficient detail that a technically trained individual not familiar with the system can successfully follow the procedures.

The full ST&E shall include both the full security control testing and the full functional or application specific functional security controls. The STE Plan shall identify all testing assumptions, constraints, and dependencies and include a proposed schedule that identifies which personnel, hardware, software, and other requirements that must be met for each portion of the schedule to accomplish full system security testing of all system security functional and assurance requirements where the requirements are not stated as being fulfilled by another system. The following test methods shall be used:

Analysis

The "analysis" verification method shall be used to appraise a process, procedure, or document to ensure properly documented actions (e.g. risk assessments, audit logs, organization level policies, etc.) are in compliance with established requirements. An example of "analysis" as an evaluation technique would be to review documented physical security policies and procedures to ensure compliance with established requirements. This verification method is often called a documentation review.

Demonstration

The contractor will randomly observe individuals to verify that activities on the system follow the documented procedure or process as the activity is performed. (Example: Observe visitors upon computer room entry in order to verify that all visitation procedures are followed.)

Interview

The contractor will interview personnel to verify that the security policies and procedures are understood as implemented and prescribed by governing policies and regulations.

Inspection

The contractor will review and analyze visitor logs to verify all information requested has been entered on the log. (Example: The contractor shall verify that the visitor's name, signature, organization, reason of visit, arrival and departure date, time, and the escort's name, initials, or signature are included on the log sheets.)

Technical Test

The "Technical Test" verification method shall be used to verify that each implemented control is functioning as intended with the contractor attempting to access a system by logging on to that system from his workstation (or other device) using an incorrect password to see if the system responds with an error message stating incorrect password or denies access after exceeding the maximum threshold for logon attempts and is directed to call the system administrator to gain access.

Testing requirements that are stated as being fulfilled by another system (provider) shall be accomplished by verifying that the provider system security plan in-place controls meet the requirement.

The STE Plan shall be documented in a report that follows the NRC Template for System Security Test and Evaluation Plan. The report shall be delivered in draft form and then in pre-Test form after NRC comments are incorporated. The NRC IT Security staff review of the draft is required to ensure compliance. The contractor shall update the STE Plan after completion of the system security test and evaluation plan test report to reflect validated information. The NRC Senior IT Security Officer must approve the final STE Plan to enable system accreditation.

The Contractor shall estimate an initial development of the ST&E plan and 1 update to the plan. The Contractor shall estimate 2 full ST&E plan executions and reports.

Subtask 9:

Full System Test and Evaluation Report

The contractor shall assist the NRC in the testing validation of the System Security Test and Evaluation Plan (STE Plan) that has been approved and signed by the NRC Senior Information Technology Security Officer (SITSO). Testing shall follow the approved test procedures documented in the STE Plan. The contractor shall document the testing in a System Security Test and Evaluation Report (STE Report). The System STE Report shall be developed in accordance with NIST SP 800-53 and 800-53A "Recommended Security Controls for Federal Information Systems," NIST SP 800-37 "Guide for the Security Certification and Accreditation of Federal Information Systems," and the NRC System Security Test and Evaluation Report Template.

The contractor shall document the results of the STE Test in a report that follows the NRC Template for System Security Test and Evaluation Report. The STE Report shall identify all testing assumptions, constraints, and dependencies as well as any anomalies, impromptu tests, and deviations encountered during testing. The STE Report shall include the actual testing schedule and detailed test results for each test procedure outlining specific errors encountered. The STE Report shall include a summary of the system scans and a table of test findings incorporating any test issues and recommendations. The STE Report shall identify any requirements that have not been met and identify the resulting impact to the system. The STE Report shall be delivered in draft form and then in final form after NRC comments are incorporated. The NRC Senior Information Technology Security Officer (SITSO) must approve the final STE Report to enable system accreditation.

The Contractor shall estimate an initial development of the ST&E plan and 1 update to the plan. The Contractor shall estimate 2 full ST&E plan executions and reports.

Subtask 10:

Security Reporting.
In addition to the applicable requirements, the contractor shall provide a Plan of Action and Milestone Status Tracking Report, FISMA Compliance and Health Report, Risk and Security Vulnerability Trending Report, Security Scoping and Categorization Report, and Security Costs Report.

Subtask 11:

Integrate Project Plan.
Microsoft Project Plan that incorporates all tasks and projects such that the individual projects roll up into an Integrated Security project schedule encompassing all NRC security related activities, services, and deliverables. The Microsoft Project Plan shall identify resources for each activity and include the Work Breakdown Structure levels.

Subtask 12:

Develop Common Control Sets and Procedures.
The contractor shall develop a standardized set of streamlined security certification and accreditation documentation that focuses on the functional alignment of common security control sets and standard operating procedures for LOW, MODERATE, and HIGH Baseline systems consistent with FISMA, and NIST Special Publication Series 800-53 that integrate with the NRC Project Management Methodology (PMM) and Enterprise Architecture (EA)

Subtask 13:

Integrated Security Activity Scheduling

Contractor staff shall develop and maintain an integrated security schedule with resource utilization in MS-Project for all NRC security related activities, services, and deliverables.

Subtask 14:

Security Technology Integration and Implementation Solutions

The contractor shall provide technical staff capable of implementing technical security solutions resulting from work identified under this contract on an as needed basis.

6.0 Meetings and Travel

Occasional travel to the NRC Headquarters offices located in Rockville, Maryland may be required. Local travel expenses will not be paid by the NRC. Parking on-site is not available.

7.0 NRC Furnished Material

NRC staff will provide copies of applicable NRC regulations, NRC Templates, and applicable guidance materials.

8.0 Contractor Acquired Material/Subcontractors

The contractor shall obtain the necessary material and specialty subcontractors as necessary to perform the work under this effort.

9.0 Schedule

The contractor shall provide final draft security documentation and reports for each system consistent with the Project Manager approved integrated project plan (Subtask 1). NRC will provide security documentation templates and examples.

The contractor shall provide final security documentation and reports for each system consistent with the Project Manager approved integrated project plan (Subtask 1). NRC will provide security documentation templates and examples.

10.0 Deliverables

The contractor shall provide the following deliverables. Deliverables shall be prepared in parallel with one another, but in order of the following sequence:

Required Service	Service Type	Standard of Performance
Project Plan (See Subtask 1)	Time and Materials	Critical
Systems Categorization (See Subtask 2)	Time and Materials	Critical
Privacy Impact Assessment (See Subtask 2)	Time and Materials	Critical
Electronic Records Disposition (See Subtask 2)	Time and Materials	Critical
SCA Plan/Execution (See Subtask 3 and 8)		
SCA Report (See Subtask 3 and 8)		
Contingency Plan (See Subtask 4)	Time and Materials	Critical
Contingency Planning Test Plan and Report (See Subtask 5)	Time and Materials	Critical

E-Authentication Risk Assessment (See Subtask 2)	Time and Materials	Critical
Risk Assessment (See Subtask 6)	Time and Materials	Critical
Systems Security Plan (SSP) (See Subtask 7)	Time and Materials	Critical
System Test and Evaluation (ST&E) Plan (See Subtask 8)	Time and Materials	Critical
System Test and Evaluation of Test Plan and Report (See Subtask 9)	Time and Materials	Critical
Security Reporting. (See Subtask 10)	Time and Materials	Critical
Integrated Security Activity Project Plan. (See Subtask 11)	Time and Materials	Critical
Development of Common Control Sets and Procedures. (See Subtask 12)	Time and Materials	Critical
Integrated Security Activity Scheduling. (See Subtask 13)	Time and Materials	Critical
Security Technology Integration and Implementation. (See Subtask 14)	Time and Materials	Non-Critical

Upon receipt of NRC comments on submitted draft reports, the contractor shall address each comment and revise the report as needed to address NRC input.

11.0 Special Business Instructions

Pricing shall be broken out **by subtask by deliverables**, with a cumulative total for all subtasks. The price quote must identify all necessary costs, including estimated labor hours, labor categories, and loaded labor rates.

12.0 Technical Direction

John Bird is designated as the Technical Monitor for this task.

The Technical Monitor is responsible for providing technical guidance to the performing organization regarding staff interpretations of technical aspects of regulatory requirements along with relevant documents when requested by the performing organization.

All work products must be reviewed and approved by the Technical Monitor before they are submitted as final documents. All technical direction given to the performing organization must be consistent with the work scope and schedule.

The Technical Monitor is not authorized to unilaterally make changes to the approved work scope or schedule or give the performing organization any direction that would increase costs over approved levels.

13.0 Performance Standards

Required Service	Service Type	Standard of Performance	Method of Surveillance	Maximum Allowable Deviation from Standard Performance
Project Plan	Time and Materials	Critical	100% Inspection by Project Officer Customer Satisfaction Survey (Council Member Reviews/Project Sponsors)	0% deviation, looking for a minimum of 100% accuracy
Systems Categorization.	Time and Materials	Critical	100% Inspection by Project Officer Customer Satisfaction Survey (Council Member Reviews/Project Sponsors)	0% deviation, looking for a minimum of 100% accuracy
Privacy Impact Assessment	Time and Materials	Critical	100% inspection by Project Officer Customer Satisfaction Survey (Council Member Reviews/Project Sponsors)	0% deviation, looking for a minimum of 100% accuracy
Electronic Records Disposition	Time and Materials	Critical	100% Inspection by Project Officer Customer Satisfaction Survey (Council Member Reviews/Project Sponsors)	0% deviation, looking for a minimum of 100% accuracy
E-Authentication Risk Assessment	Time and Materials	Critical	100% Inspection by Project Officer/Customer Satisfaction Survey (Council Member Reviews/Project Sponsors)	0% deviation, looking for a minimum of 100% accuracy
Risk Assessment	Time and Materials	Critical	100% Inspection by Project Officer Customer Satisfaction Survey (Council Member Reviews/Project Sponsors)	0% deviation, looking for a minimum of 100% accuracy
Systems Security Plan (SSP)	Time and Materials	Critical	100% Inspection by Project Officer	0% deviation, looking for a minimum of 100% accuracy
SCA Plan	Time and	Critical	100% Inspection by	0% deviation, looking for

	Materials		Project Officer	a minimum of 100% accuracy
SCA Report	Time and Materials	Critical	100% Inspection by Project Officer	0% deviation, looking for a minimum of 100% accuracy
Contingency Plan	Time and Materials	Critical	100% Inspection by Project Officer Customer Satisfaction Survey (Council Member Reviews/Project Sponsors)	0% deviation, looking for a minimum of 100% accuracy
Contingency Planning Test Plan and Report	Time and Materials	Critical	100% Inspection by Project Officer	0% deviation, looking for a minimum of 100% accuracy
System Test and Evaluation (ST&E) Plan	Time and Materials	Critical	100% Inspection by Project Officer Customer Satisfaction Survey (Council Member Reviews/Project Sponsors)	0% deviation, looking for a minimum of 100% accuracy
System Test and Evaluation of Test Plan and Report	Time and Materials	Critical	100% Inspection by Project Officer	0% deviation, looking for a minimum of 100% accuracy
Security Reporting.	Time and Materials	Critical	100% Inspection by Project Officer Customer Satisfaction Survey (Council Member Reviews/Project Sponsors)	0% deviation, looking for a minimum of 100% accuracy
Integrated Security Activity Project Plan.	Time and Materials	Critical	Customer Satisfaction Survey (Council Member Reviews/Project Sponsors, Staff, and volunteers)	0% deviation, looking for a minimum of 100% accuracy
Development of Common Control Sets and Procedures.	Time and Materials	Critical	100 Inspection by Project Officer Customer Satisfaction Survey	0% deviation, looking for a minimum of 100% accuracy
Integrated Security Activity Scheduling.	Time and Materials	Critical	Customer Satisfaction Survey (Council Member Reviews/Project Sponsors, Staff, and volunteers)	0% deviation, looking for a minimum of 100% accuracy
Security Technology Integration and	Time and Materials	Non-Critical	Customer Satisfaction Survey (Council Member Reviews/Project	0% deviation, looking for a minimum of 100% accuracy

Implementation.			Sponsors, Staff, and volunteers)	

NOTE: There shall be no cost corrective actions. Indefinite task/delivery orders will set forth the applicable standards.

*See contract for a description of performance standards.