ORDER FOR SUPPLIES OR SERVICES

PAGE OF PAGES: 1 of 8

IMPORTANT: Mark all packages and papers with contract and/or order numbers. BPA NO.

1. DATE OF ORDER: SEP 25 2006	2. CONTRACT NO. (If any): GS35F0229K
3. ORDER NO.: DR-33-06-317-T010 MODIFICATION NO.:	4. REQUISITION/REFERENCE NO.:

5. ISSUING OFFICE (Address correspondence to):
U.S. Nuclear Regulatory Commission
Div. of Contracts
Attn: CMB3
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-6-F-41
11545 Rockville Pike
c. CITY: Washington | d. STATE: DC | e. ZIP CODE: 20555

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

f. SHIP VIA:

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:
6-7N15-5H2357 N7235 252A 31X020 FFS# CFO06410
OBLIGATE: $162,660.38

10. REQUISITIONING OFFICE: 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		14. GOVERNMENT B/L NO.	15. DELIVER TO F.O.B. POINT ON OR BEFORE (Date)	16. DISCOUNT TERMS
a. INSPECTION	b. ACCEPTANCE			
Rockville, MD	Rockville, MD		9/24/2007	NET 30

17. SCHEDULE (See reverse for Rejections)

ITEM NO. (A)	SUPPLIES OR SERVICES (B)	QUANTITY ORDERED (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)	QUANTITY ACCEPTED (G)
	TASK ORDER 10 UNDER NRC ORDER DR-33-06-317 (CISSS): The Contractor shall provide the U.S. Nuclear Regulatory Commission with, "Major/High Systems C&A: Human Resource Management System (HRMS) Modernization," services in accordance with the following: - The attached Statement of Work - The attached Schedule of Supplies and Services and Prices - The terms and conditions of GSA Contract GS-35F-0229K - The terms and conditions of NRC Order DR-33-06-317 Reference: MAR Quotation (Ref #2006-090-WA971), dtd 9/18/06 DUNS: 062021639 ACCEPTANCE: Linda Klages 09/21/2006 Signature Date Linda Klages, Vice President, Contracts Print Name/Title					

SEE BILLING INSTRUCTIONS ON REVERSE	18. SHIPPING POINT	19. GROSS SHIPPING WEIGHT	20. INVOICE NO.	$162,660.38
	21. MAIL INVOICE TO:			17(h) TOTAL (Cont. pages)
	a. NAME: U.S. Nuclear Regulatory Commission Payment Team, Mail Stop T-7-I-2			
	b. STREET ADDRESS (or P.O. Box): Attn: DR-33-06-317-T010			17(i). GRAND TOTAL
	c. CITY: Washington	d. STATE: DC	e. ZIP CODE: 20555	$162,660.38

22. UNITED STATES OF AMERICA BY (Signature): Eleni Jernell

23. NAME (Typed): Eleni Jernell
Contracting Officer
TITLE: CONTRACTING/ORDERING OFFICER

AUTHORIZED FOR LOCAL REPRODUCTION
PREVIOUS EDITION NOT USABLE
TEMPLATE - ADM001

SUNSI REVIEW COMPLETE

OPTIONAL FORM 347 (REV. 3/2005)
PRESCRIBED BY GSA/FAR 48 CFR 53.213(e)
ADM002

DELIVERY ORDER DR-33-06-317
TASK ORDER 10 (T010)
MAJOR/HIGH SYSTEMS C&A: HUMAN RESOURCE MANAGEMENT SYSTEM (HRMS) MODERNIZATION

1.0 OBJECTIVE

The Contractor shall support the OIS in certification and accreditation of major information systems 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 SOW ENCLOSURE 6 of Delivery Order DR-33-06-317, entitled, "C&A PROCESS AND DELIVERABLES" such that an Authorization to Operate (ATO) which confers full accreditation shall be granted the system. The Contractor shall perform these security support tasks specified for a HIGH security baseline systems.

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.

2.0 SCOPE OF WORK

The Contractor shall provide security analyst staff and develop all requisite systems certification and accreditation documentation such that the Human Resource Management System (HRMS Modernization) obtains an Authorization to Operate (ATO) and no system crosses fiscal year boundaries with an Interim Authorization to Operate (IATO).

System Name: Human Resource Management System (HRMS Modernization)

Sponsor Office: Office of the Chief Financial Officer (OCFO)

System Owner: Director, OCFO

System Description: The Human Resources Management System (HRMS) Time and Labor (T&L) Module is the agency's system for capturing time, attendance, and labor data. It is the system that employees use to enter their time.

Status: HRMS Modernization is considered a new development effort.

The Contractor shall provide security analyst staff and the development of the associated documentation associated with the security support tasks specified below for classified and unclassified LOW, MODERATE, and HIGH security baseline systems for the system category "Major Application", as specified in SOW ENCLOSURE 6 of Delivery Order DR-33-06-317 - C&A PROCESS AND DELIVERABLES.

The term "Major Application" (MA) 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 an 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.

3.0 PERIOD OF PEFORMANCE

The period of performance of this task order is September 25, 2006 through September 24, 2007.

4.0 FUNDING

(a) The total estimated amount (ceiling) for the products/services ordered, delivered, and accepted under this task order is $162,660.38.

(b) The amount presently obligated with respect to this task order is **$162,660.38**. The Contractor shall not be obligated to incur costs above this ceiling/obligated amount unless and until the Contracting Officer shall increase the amount obligated. When and if the amount(s) paid and payable to the Contractor hereunder shall equal the obligated amount, the Contractor shall not be obligated to continue performance of the work unless and until the Contracting Officer shall increase the amount obligated with respect to this contract. Any work undertaken by the Contractor in excess of the obligated amount specified above is done so at the Contractor's sole risk.

5.0 TRAVEL

No travel is required.

6.0 SCHEDULE

The Contractor shall provide final draft security documentation and reports for each system consistent with the NRC-approved integrated project plan (Subtask 1).

7.0 SPECIFIC TASKS

The Contractor shall support the NRC C&A of HRMS Modernization system and application service provider facility as described below:

Subtask 1: Integrated Security Activity Project Plan.

Develop and implement a project plan to ensure completion of the HRMS Modernization certification and accreditation tasks within the period of performance. The Contractor shall be required to develop and maintain an Integrated Security Activity Project Plan and perform Integrated Activity Scheduling for the program. These deliverables shall be developed at the individual project level (i.e., each system for which a certification and accreditation effort will be undertaken) and aggregate to the program level. The Microsoft Project Plan shall incorporate 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. The project plan will include:

- A Level 5 **Work Breakdown Structure (WBS)**. The WBS shall include a definition of the work to be conducted decomposed into distinct discrete manageable tasks or groups of tasks (work packages) with decisive outputs and specific measurable entry and exit criteria. Each work package shall have a short duration, or can be divided into a series of milestones whose status can be objectively measured. Each work package shall be assigned a start and finish date, a budget value, and can be integrated with higher-level schedules.
- A **schedule and budget** for accomplishing the work identifying what resources are needed and how much effort will be required in what time frame to complete each of the tasks in the WBS. The Contractor shall allocate a portion of the budget for each work package that comprises the WBS, and ensure that the WBS adequately defines all work necessary to meet the requirements for the project.

Subtask 2: 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 system configuration assessments, security scans and penetration tests;
- 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; and,
- 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 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 3: Systems Security Plan (SSP)

The security plan shall be developed in accordance with NIST SP 800-53 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 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 SITSO must approve the final to enable system accreditation.

Subtask 4: Systems Security Controls and Security Requirements Support.

The Contractor shall support the NRC staff in the development and documentation of security controls and security requirements and associated technical resolutions, risk mitigation, and implementations within the Rational Suite Enterprise.

Subtask 5: Review, Verification, and Validation of Security Controls and Requirements.

The Contractor shall review, verify, and validate all security controls and security requirements and associated technical resolutions, risk mitigation, and implementations contained within various NRC security and systems development documentation or the Rational Suite Enterprise such that confirmation that the system and associated controls are operating as intended.

Subtask 6: Systems Security Controls and Security Requirements Test Plan Development Support.

The Contractor shall support the NRC staff in the development and documentation of a test plan within the Rational Suite Enterprise that exercises the systems security controls and security requirements and associated technical resolutions, risk mitigation, and implementations such that confirmation that the system and associated controls are operating as intended and in accordance with NIST SP 800-53A, NIST SP 800-53 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 ST&E 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 observe randomly 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 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.

Subtask 7: Review, Verification, and Validation of Security Controls and Requirements Test Plan and Test Plan Execution.

The Contractor shall independently review, verify, and validate all systems security test plans and procedures to ensure the accuracy and adequacy of documented test procedures for all systems security controls and security requirements and associated technical resolutions, risk mitigation, and implementations contained within various NRC security and systems development documentation or the Rational Suite Enterprise such that confirmation that the system and associated controls are operating as intended. The Contractor shall update the ST&E 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 to enable system accreditation.

Subtask 8: Contingency Plan.

The Contractor shall support the NRC staff in the development and documentation of a contingency plan and test procedures within the Rational Suite Enterprise. 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 to enable system accreditation.

Subtask 9: 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 developed and documented by the Contractor within the Rational Suite Enterprise. 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 the 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 10: Quarterly Penetration and Vulnerability Scanning.

The Contractor shall perform quarterly analysis, penetration, vulnerability, configuration, systems integrity, and patch management scans. The Contractor shall identify, analyze, and propose tested corrective actions that ensure the currency of the systems security posture and ensures that controls are operating as intended.

Subtask 11: Annual Analysis of Systems Documentation, Security Controls, Requirements, and Implementation Status.

The Contractor shall conduct on all Major Application and GSS NRC systems an inclusive independent audit annually that shall include but is not limited to the review, verification, and validation of all current systems documentation, analysis, penetration, vulnerability, configuration, systems integrity, and patch management scans. The Contractor shall identify, analyze, and propose tested corrective actions that ensure the currency of the systems security posture and ensures that controls are operating as intended. The Contractor shall identify NRC information systems security vulnerability trends at an agency and system level with special attention to those deficiencies that would impact NRC FISMA compliance.

GSA CONTRACT: GS-35F-0229K
DELIVERY/TASK ORDER NO: DR-33-06-317
TASK ORDER NO: DR-33-06-317-T010
TASK ORDER TITLE: MAJOR/HIGH SYSTEMS C&A:
HUMAN RESOURCE MANAGEMENT SYSTEM (HRMS) MODERNIZATION

SCHEDULE OF SUPPLIES OR SERVICES AND PRICE/COST

TASK ORDER 10 CEILING $ 162,660.38

	SOW REF	DELIVERABLE TITLE AND REQUIRED LABOR CATEGORIES FOR COMPLETION OF 1 DELIVERABLE FOR 1 SYSTEM	DISCOUNTED GSA LABOR RATE	HOURS FOR MAJOR SYSTEM	TOTAL AMOUNT FOR MAJOR SYSTEM
				T-S HIGH ONLY	
26	Encl 6	**FULL C&A PACKAGE (1 SYSTEM)**			
		Project Manager	$ 119.37	40	$ 4,774.64
		QA Manager	$ 115.69	16	$ 1,851.09
		Security Specialist IV	$ 141.40	80	$ 11,312.22
		Security Specialist II	$ 119.37	1000	$ 119,366.00
		Documentation Specialist	$ 78.85	40	$ 3,154.18
		Technical Writer II	$ 58.20	200	$ 11,639.84
		Sr. Information Engineer	$ 88.02	120	$ 10,562.40
		TOTALS FOR FULL C&A PACKAGE (1 SYSTEM)		**1496**	**$ 162,660.38**