ORDER FOR SUPPLIES OR SERVICES

PAGE OF PAGES: 1 | 6

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

1. DATE OF ORDER: SEP 15 2006	2. CONTRACT NO. (If any): GS35F0229K
3. ORDER NO.: DR-33-06-317-T004 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
b. STREET ADDRESS:
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: $88,589.31

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		9/14/2007	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 4 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 Resources Management System (HRMS) - Legacy" services in accordance with the following: - The attached Statement of Work - The attached Schedule of Supplies or 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 # 2006-082/WA971), dtd 8/22/06 DUNS: 062021639 ACCEPTANCE: Linda Klages 09/15/2006 Signature Date Linda Klages, VP, Contracts, MAR, Inc. Print Name/Title					

SEE BILLING INSTRUCTIONS ON REVERSE	18. SHIPPING POINT	19. GROSS SHIPPING WEIGHT	20. INVOICE NO.	$88,589.31
	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-T004			17(i). GRAND TOTAL
	c. CITY: Washington	d. STATE: DC	e. ZIP CODE: 20555	$88,589.31

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 - ADM002

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 4 (T004)
MAJOR/HIGH SYSTEMS C&A: HUMAN RESOURCES MANAGEMENT SYSTEM (HRMS) - LEGACY

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 HRMS system obtains an Authorization to Operate (ATO) and no system crosses fiscal year boundaries with an Interim Authorization to Operate (IATO).

System Name: Human Resources Management System (HRMS) - Legacy

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 is currently operating under an interim approval to operate that expires on November 30, 2007. The status matrix below indicates the current (as of 8/15/06) HRMS ISS C&A progress:

HRMS Certification and Accreditation Status

	ATO Expiration	Monthly Status Report (System Owner)	PIA (System Owner)	NRC FORM 616 (System Owner)	NRC FORM 637 (System Owner)	E-Authentication Risk Assessment	MOU (System Owner)	ISA (System Owner)	Security Categorization	C&A Schedule (System Owner)	Risk Assessment	System Security Plan	ST&E Test Procedure Report	ST&E Test Procedure Execution Report	Corrective Action Plan	ATO Memo (System Owner)	Contingency Plan Test Procedures Report	Contingency Plan Test Procedure Execution Report
HRMS System Owner OCFO	06/31/07	06/06/06	06/03/06	07/21/06	06/21/06	12/12/06	07/13/06	07/15/06	02/07/06	02/07/06	07/14/06	06/17/06	06/01/06	05/15/06	05/15/06	10/25/06	1?/06	1?/06
Certified	Package Submitted (PENDING SITSC/DAA APPROVAL)			Submitted to SITSC	Documents Finalized						In Progress		Re-Work Required			Milestone Overdue		

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 15, 2006 through September 14, 2007.

4.0 FUNDING

(a) The total estimated amount (ceiling) for the products/services ordered, delivered, and accepted under this task order is $88,589.31.

(b) The amount presently obligated with respect to this task order is **$88,589.31**. 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 anticipated under this Task Order.

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 as described below:

Subtask 1: Integrated Security Activity Project Plan.

Develop and implement a project plan to ensure completion of the HRMS 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: 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 3: 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 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 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 4: 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.

GSA CONTRACT: GS-35F-0229K
DELIVERY/TASK ORDER NO: DR-33-06-317
TASK ORDER NO: DR-33-06-317-T004
TASK ORDER TITLE: MAJOR/HIGH SYSTEMS C&A: HUMAN RESOURCES MANAGEMENT SYSTEM (HRMS) - LEGACY

SCHEDULE OF SUPPLIES OR SERVICES AND PRICE/COST

TASK ORDER 4 CEILING $ 88,589.31

	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
				HIGH ONLY	
20	Encl 6	**SYSTEM SECURITY PLAN (1 SYSTEM)**			
		Project Manager	$ 119.37	8	$ 954.93
		QA Manager	$ 115.69	8	$ 925.55
		Security Specialist III	$ 124.88	40	$ 4,995.01
		Security Specialist II	$ 119.37	200	$ 23,873.20
		Technical Writer II	$ 58.20	64	$ 3,724.75
		TOTALS FOR SYSTEM SECURITY PLAN (1 SYSTEM)		**320**	**$ 34,473.43**
21	Encl 6	**ST&E PROCEDURES PLAN (1 SYSTEM)**			
		Project Manager	$ 119.37	16	$ 1,909.86
		QA Manager	$ 115.69	8	$ 925.55
		Security Specialist III	$ 124.88	16	$ 1,998.00
		Security Specialist II	$ 119.37	160	$ 19,098.56
		Technical Writer II	$ 58.20	40	$ 2,327.97
		TOTALS FOR ST&E PROCEDURES PLAN (1 SYSTEM)		**240**	**$ 26,259.93**
22	Encl 6	**ST&E EXECUTION REPORT (1 SYSTEM)**			
		Project Manager	$ 119.37	8	$ 954.93
		QA Manager	$ 115.69	8	$ 925.55
		Security Specialist III	$ 124.88	16	$ 1,998.00
		Security Specialist II	$ 119.37	160	$ 19,098.56
		Technical Writer II	$ 58.20	40	$ 2,327.97
		Network Security Analyst	$ 63.77	40	$ 2,550.94
		TOTALS FOR ST&E EXECUTION REPORT (1 SYSTEM)		**272**	**$ 27,855.94**

TOTAL $ 88,589.31