

**ORDER FOR SUPPLIES OR SERVICES**

**IMPORTANT: Mark all packages and papers with contract and/or order numbers.**

BPA NO.

1. DATE OF ORDER <b>SEP 19 2006</b>		2. CONTRACT NO. (If any) GS35F0229K		6. SHIP TO:	
3. ORDER NO. DR-33-06-317-T003		4. REQUISITION/REFERENCE NO.		a. NAME OF CONSIGNEE U.S. Nuclear Regulatory Commission	
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				b. STREET ADDRESS Two White Flint North - MS T-6-C-30 Attn: Carl Konzman	
7. TO:		c. CITY Washington		d. STATE DC	e. ZIP CODE 20555
a. NAME OF CONTRACTOR MAR, INCORPORATED		f. SHIP VIA			
b. COMPANY NAME		8. TYPE OF ORDER			
c. STREET ADDRESS 1803 RESEARCH BLVD SUITE 204		e. STATE MD		i. ZIP CODE 208506106	
d. CITY ROCKVILLE		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.			
9. ACCOUNTING AND APPROPRIATION DATA 660-15-111-160 N6357 252A 31X0200.660 FFS#: RES-C06-027 OBLIGATE: \$247,086.88		10. REQUISITIONING OFFICE OIS/BPIAD/ADMB			
11. BUSINESS CLASSIFICATION (Check appropriate box(es)) <input checked="" type="checkbox"/> a. SMALL <input type="checkbox"/> b. OTHER THAN SMALL <input type="checkbox"/> c. DISADVANTAGED <input type="checkbox"/> g. SERVICE-DISABLED VETERAN-OWNED <input type="checkbox"/> d. WOMEN-OWNED <input type="checkbox"/> e. HUBZone <input type="checkbox"/> 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) 9/18/2007	
a. INSPECTION Rockville, MD	b. ACCEPTANCE Rockville, MD			16. DISCOUNT TERMS 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)
	<p>TASK ORDER 3 UNDER DR-33-06-317 (CISS): The Contractor shall provide the U.S. Nuclear Regulatory Commission with, "RES ISS Program Support" services in accordance with the following:</p> <ul style="list-style-type: none"> <li>- The attached Statement of Work</li> <li>- The attached Schedule of Supplies or Services and Prices</li> <li>- The terms and conditions of GSA Schedule GS-35F-0229K</li> <li>- The terms and conditions of NRC Order DR-33-06-317</li> </ul> <p>Reference: MAR Quotation (Ref # 2006-081/WA971), dtd 9/13/06</p> <p>DUNS: 062021639</p> <p>ACCEPTANCE:</p> <p align="right"><i>Linda Klages</i>      9/19/2006 Signature      Date</p> <p>Linda Klages Vice President, Contracts</p> <p>Print Name/Title</p>					

SEE BILLING INSTRUCTIONS ON REVERSE	18. SHIPPING POINT		19. GROSS SHIPPING WEIGHT		20. INVOICE NO.		17(h) TOTAL (Cont. pages)
	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: DR-33-06-317-T003						
c. CITY Washington		d. STATE DC	e. ZIP CODE 20555		\$247,086.88		17(i) GRAND TOTAL
22. UNITED STATES OF AMERICA BY (Signature) <i>Eleni Jernell</i>					23. NAME (Typed) Eleni Jernell Contracting Officer TITLE: CONTRACTING/ORDERING OFFICER		

**DELIVERY ORDER DR-33-06-317  
TASK ORDER 3 (T003)  
RES ISS PROGRAM SUPPORT**

**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 under 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.

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

Contractor shall provide a 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 Delivery Order DR-33-06-317 SOW ENCLOSURE 6 - C&A PROCESS AND DELIVERABLES.

**3.0 PERIOD OF PERFORMANCE**

The period of performance of this task order is September 19, 2006 through September 18, 2007.

**4.0 FUNDING**

- (a) The total estimated amount (ceiling) for the products/services ordered, delivered, and accepted under this task order is \$247,086.88.
- (b) The amount presently obligated with respect to this task order is **\$247,086.88**. 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.

## 7.0 SPECIFIC TASKS

The Contractor shall provide annual support to the NRC's Office of Research that will assist in the development of an ISS program for this Office. The Contractor shall support the NRC as described below:

### **Subtask 1: Development, Update and Maintenance of 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 a MODERATE, and HIGH Baseline systems consistent with FISMA, and NIST SP 800-53 that integrate with the NRC PMM and EA within the Rational Suite Enterprise.

### **Subtask 2: Security Program Communications Support.**

The Contractor shall support the NRC in communicating the ISS program's processes and on the use of the associated information systems tools. The Contractor shall utilize the Rational Method Composer to develop Intranet, web based process flows and procedures.

### **Subtask 3: System Security Controls and Security Requirements Support.**

System 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. Including the following:

#### **Security Engineering and Common Security Controls Support**

Security Engineering and Common Security Controls Support: The Contractor shall provide Security Engineering support for application development and information systems solution assessment and proposal such that information systems architectures proposed for implementation at the NRC are based on sound security engineering principles and practices. The contract shall support the NRC enterprise architecture staff in the development of the security line of business program and documentation, and support the NRC in the assessment, documentation, and implementation of common security solutions and OMB information systems security line of business integration.

#### **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.

#### **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.

#### **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.

### **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.

### **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.