ORDER FOR SUPPLIES OR SERVICES

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

1. DATE OF ORDER: APR 22 2008	2. CONTRACT NO. (If any): GS35F0229K
3. ORDER NO.: DR-33-06-317-T044 MODIFICATION NO.	4. REQUISITION/REFERENCE NO.: OIS-06-317 dtd: 4/11/08
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: Attn: Bill Dabbs, 11545 Rockville Pike, Mail Stop: T-2-C-2		
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 RESEARCH 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 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
B&R:810-15-5E1-330 JC:J1296 BOC:252A APP:31X0200.810
FFS:10870649C OBLIGATE: $150,000.00

10. REQUISITIONING OFFICE: CIO CSO

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 SMALLBUSINESS

12. F.O.B. POINT: Destination

13. PLACE OF a. INSPECTION	13. PLACE OF b. ACCEPTANCE	14. GOVERNMENT B/L NO.	15. DELIVER TO F.O.B. POINT ON OR BEFORE (Date)	16. DISCOUNT TERMS
Rockville, MD	Rockville, MD		See SOW	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 44 UNDER NRC ORDER DR-33-06-317 (CISSS): The contractor shall provide the U.S. Nuclear Regulatory Commission with, "Office of Information Services (OIS) Infrastructure Computer Operations Division (ICOD) Contingency Planning" services in accordance with the following: - The attached Statement of Work (SOW) - The attached Schedule of Supplies or Services and Price/Cost - The terms and conditions of GSA Schedule GS-35F-0229K - The terms and conditions of NRC Order DR-33-06-317 Reference: MAR Quotation (Ref# 2008-051/WA971), dtd 4/14/08 DUNS: 062021639 ACCEPTANCE: Linda Klages 4/29/2008 Signature Date Linda Klages, Vice President, Contracts Print Name/Title					

18. SHIPPING POINT	19. GROSS SHIPPING WEIGHT	20. INVOICE NO.	17(h) TOTAL (Cont. pages)
			$292,741.11 (Ceiling)

SEE BILLING INSTRUCTIONS ON REVERSE

21. MAIL INVOICE TO:

a. NAME: U.S. Nuclear Regulatory Commission, Division of Contracts, Mail Stop T-7-I-2			
b. STREET ADDRESS (or P.O. Box): Attn: DR-33-06-317-T044			17(i). GRAND TOTAL: $292,741.11
c. CITY: Washington	d. STATE: DC	e. ZIP CODE: 20555	

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

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

DELIVERY ORDER NO. DR-33-06-317

TASK ORDER NO. 44

OFFICE OF INFORMATION SERVICES (OIS) INFRASTRUCTURE COMPUTER OPERATIONS DIVISION (ICOD) CONTINGENCY PLANNING

1.0 OBJECTIVE

The contractor shall assist the Computer Security Office (CSO) with the development, verification, and validation of the Contingency Planning Process for the following Office of Information Services (OIS) Infrastructure Computer Operations Division (ICOD) Automated Information Systems (AIS):

1. Windows Infrastructure Services (WINDOWS) — Sensitivity High
2. Novell Server Infrastructure (NOVELL) — Sensitivity Moderate
3. Managed Desktops and Laptops (DESKTOPS) — Sensitivity High
4. Telecommunications (TELCOMM) — Sensitivity High
5. Intrusion Detection System and Security Devices (IDSSD) — Sensitivity Moderate
6. Managed Public Key Infrastructure (MPKI) — Sensitivity Moderate

2.0 BACKGROUND

The following summarizes the systems that the contractor will be working with:

1. Please refer to the current WINDOWS Security Categorization document (ML063620601) for a description of the system boundaries and scope.
2. Please refer to the current NOVELL Security Categorization document (ML063540468) for a description of the system boundaries and scope.
3. Please refer to the current DESKTOPS Security Categorization document (ML063620602) for a description of the system boundaries and scope.
4. Please refer to the current TELCOMM Security Categorization document (ML063480217) for a description of the system boundaries and scope.
5. Please refer to the current IDSSD Security Categorization document (ML063480043) for a description of the system boundaries and scope.
6. Please refer to the current MPKI Security Categorization document (ML060450565) for a description of the system boundaries and scope

3.0 SCOPE OF WORK

The contractor must ensure the system's contingency planning process has been implemented according to federally mandated and Nuclear Regulatory Commission (NRC) defined security requirements. The contractor will identify any deficiencies and will specify any operational risks that may affect the system's ability to perform its mission and protect its data (both stored and transmitted). The contractor shall perform the following:

Tasks	WINDOWS	NOVELL	DESKTOPS	TELCOMM	IDSSD	MPKI
Subtask 2 – Contingency Plan (CP)	Shall work with the system owner to develop the system's CP. This includes the business impact assessment (BIA).	Shall work with the system owner to develop the system's CP. This includes the business impact assessment (BIA).	Shall work with the system owner to develop the system's CP. This includes the business impact assessment (BIA).	Shall work with the system owner to develop the system's CP. This includes the business impact assessment (BIA).	Shall work with the system owner to develop the system's CP. This includes the business impact assessment (BIA).	Shall work with the system owner to develop the system's CP. This includes the business impact assessment (BIA).
Subtask 3 – Contingency Test and Report	Shall work with the system owner to verify, validate, and document the results of the system's contingency test. Upon completion of the Contingency Test, the contractor shall update the system's CP to reflect validated information.	Shall work with the system owner to verify, validate, and document the results of the system's contingency test. Upon completion of the Contingency Test, the contractor shall update the system's CP to reflect validated information.	Shall work with the system owner to verify, validate, and document the results of the system's contingency test. Upon completion of the Contingency Test, the contractor shall update the system's CP to reflect validated information.	Shall work with the system owner to verify, validate, and document the results of the system's contingency test. Upon completion of the Contingency Test, the contractor shall update the system's CP to reflect validated information.	Shall work with the system owner to verify, validate, and document the results of the system's contingency test. Upon completion of the Contingency Test, the contractor shall update the system's CP to reflect validated information.	Shall work with the system owner to verify, validate, and document the results of the system's contingency test. Upon completion of the Contingency Test, the contractor shall update the system's CP to reflect validated information.

The contractor shall ensure that the steps, templates, and reports outlining system's the Contingency Planning process in NRC's Project Management Methodology are utilized and followed.

The contractor shall provide the necessary security support staff to develop the associated documentation to support the tasks specified in Statement of Work (SOW) ENCLOSURE 6 of Delivery Order DR-33-06-317 "CERTIFICATION AND ACCREDITATION PROCESS AND DELIVERABLES" for unclassified systems.

4.0 PERIOD OF PERFORMANCE

The period of performance of this task order will be from April 23, 2008, through April 22, 2009.

5.0 FUNDING

(a) The total estimated amount (ceiling) for the products/services ordered, delivered, and accepted under this task order is **$279,061.11** (includes $13,680.00 for NTE travel).

(b) The amount presently obligated with respect to this task order is **$150,000.00.** 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.

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 TASKS

The contractor shall support the development, verification, and validation of the Contingency Planning Process for OIS/ICOD systems according to item 23, Contingency Plan, and item 24, Contingency Plan Report, in the SOW Enclosure 6 and Section B "Schedule of Supplies or Services and Prices".

Subtask 1: Integrated Security Activity Project Plan

The contractor shall develop and implement a project plan to ensure the completion of the tasks identified in this SOW occurs as expected. The contractor shall be required to develop and maintain an Integrated Security Activity Project Plan and perform Integrated Activity Scheduling. 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 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 Project Plan shall identify resources for each activity and include the Work Breakdown Structure levels. The Project Plan will include:

- **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.

- **Schedule and Budget**

  The schedule and budget will identify what resources are needed, identify how much effort is required, and when each of the tasks specified in the WBS can be completed. 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: System CP

The Contractor shall support the NRC staff in the development and documentation of a CP and test procedures within the Rational Suite Enterprise. The System CP shall be documented in a report generated from the Rational Suite Enterprise that follows the NRC Template for the System CP. The Plan shall be maintained in its hard copy form for contingency execution should the Rational Suite Enterprise or NRC Network Infrastructure be unavailable.

The CP shall be developed in accordance with federally mandated requirements, NRC defined security requirements, National Institute of Standards & Technology (NIST) Special Publication (SP) 800-34 "Contingency Planning Guide for Information Technology Systems", NIST SP 800-37 "Guide for the Security Certification & Accreditation of Federal Information Systems", and the NRC Contingency Plan (CP) Template.

The Contractor shall provide detailed procedures for the Notification/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 CP shall contain

- Sufficient contact information (personnel and vendor)
- Equipment (hardware and software)
- Specification information to enable reconstitution of the system from scratch, all service level agreements, memoranda of understanding
- 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.
- References to the appropriate continuity of operations plan.

The System CP shall be documented in a report generated from the Rational Suite Enterprise that follows the NRC Template for System CP. The report shall be delivered in draft form and then in pre-Test form after NRC comments have been incorporated. The NRC CSO staff review of the draft is required to ensure compliance.

Subtask 3: Contingency Test and Report

The Contractor shall provide expert advice and support during the Contingency Planning Test to ensure the test plan documentation is compliant with the System CP that has been approved by the NRC. 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 federally mandated requirements, NRC defined security requirements, 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 must approve the final CP Test Report.

The Contractor shall update the system's CP once the CP Test Report has been completed to reflect validated information. The NRC must approve the final version of the system's CP.

8.0 TRAVEL

The contingency tests will be combined into one or two tests. The contractor will be required to travel to the NRC Region IV office in Arlington, Texas three times to support this effort.

U.S. NRC Region IV
Texas Health Resources Tower
611 Ryan Plaza, Suite 400
Arlington, TX 76011-4005

A not-to-exceed (NTE) line item of $13,680.00 has been included for travel required for this effort. All travel will be reimbursed in accordance with DR-33-06-317, Section 4.3, Travel Requirements.

9.0 MEETINGS

The contractor's technical representative shall attend monthly status meetings at NRC Headquarters to discuss work being done under this task order.

10.0 LEVEL OF EFFORT

The estimated level of effort for this task order is 2,484 staff hours.