

**ORDER FOR SUPPLIES OR SERVICES**

PAGE OF PAGES  
1 7

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

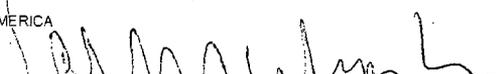
BPA NO.

1. DATE OF ORDER <b>JUN 14 2007</b>		2. CONTRACT NO. (if any) GS35F0229K		6. SHIP TO:			
3. ORDER NO. <b>DR-33-06-317-T032</b>		MODIFICATION NO.		a. NAME OF CONSIGNEE U.S. Nuclear Regulatory Commission			
4. REQUISITION/REFERENCE NO. OIS-06-317-47 FFS# 10770742C		b. STREET ADDRESS Attn: Tu Tran Two White Flint North - MS T-6-C32M				c. CITY Washington	
5. ISSUING OFFICE (Address correspondence to) U.S. Nuclear Regulatory Commission Div. of Contracts Attn: Jaye Seay, CMB3 Mail Stop T-7-I-2 Washington, DC 20555		7. TO:		d. STATE DC		e. ZIP CODE 20555	
a. NAME OF CONTRACTOR MAR, INCORPORATED		b. COMPANY NAME		f. SHIP VIA			
c. STREET ADDRESS 1803 RESEARCH BLVD SUITE 204		d. CITY ROCKVILLE		e. STATE MD		f. ZIP CODE 208506106	
9. ACCOUNTING AND APPROPRIATION DATA 710-15-5F1-340 J1259 252A 31X0200.710 OBLIGATE: 214,604.00 FFS# 10770742C		\$214,604.00		10. REQUISITIONING OFFICE CIO OIS/BPIAD/BASB			
11. BUSINESS CLASSIFICATION (Check appropriate box(es))						12. F.O.B. POINT Destination	
<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 SMALLBUSINESS			
13. PLACE OF		14. GOVERNMENT B/L NO.		15. DELIVER TO F.O.B. POINT ON OR BEFORE (Date) 8/15/2007		16. DISCOUNT TERMS NET 30	
a. INSPECTION Rockville, MD		b. ACCEPTANCE Rockville, MD					

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)
	TASK ORDER 32 UNDER NRC ORDER DR-33-06-317 (CISSS): The Contractor shall provide the U.S. Nuclear Regulatory Commission with, "Annual Analysis - Security Self Assessment 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 Schedule GS-35F-0229K - The terms and conditions of NRC Order DR-33-06-317 (See continuation page)  Reference: MAR Quotation (Ref# 2007-053/WA971), dtd 5/30/07,  DUNS: 062021639 ACCEPTANCE:  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)
21. MAIL INVOICE TO:						
a. NAME U.S. Nuclear Regulatory Commission Div of Contracts, Mail Stop T-7-I-2						17(i) GRAND TOTAL
b. STREET ADDRESS (or P.O. Box) Attn: DR-33-06-317-T032						
c. CITY Washington		d. STATE DC		e. ZIP CODE 20555		
						\$214,604.00

22. UNITED STATES OF AMERICA BY (Signature) 		23. NAME (Typed) Valerie Whipple Contracting Officer TITLE: CONTRACTING/ORDERING OFFICER	
---	--	---	--

**ORDER FOR SUPPLIES OR SERVICES  
SCHEDULE - CONTINUATION**

PAGE NO.  
2

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

DATE OF ORDER	CONTRACT NO. GS35F0229K	ORDER NO. DR-33-06-317-T032
---------------	----------------------------	--------------------------------

ITEM NO. (A)	SUPPLIES OR SERVICES (B)	QUANTITY ORDERED (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)	QUANTITY ACCEPTED (G)
	<p><u>Supplies or Services continued</u></p> <p>An email authorization to begin performance was given on June 1, 2007, with a not to exceed (NTE) ceiling price of \$25,000.00. This action definitizes the email authorization sent on June 1, 2007. The ceiling price of this Task Order is <b>\$218,290.79</b>, which is inclusive of the \$25,000.00 temporary ceiling authorized on June 1, 2007.</p>					

TOTAL CARRIED FORWARD TO 1ST PAGE (ITEM 17(H))

**DELIVERY ORDER DR-33-06-317  
TASK ORDER 32  
ANNUAL ANALYSIS - SECURITY SELF ASSESSMENT SERVICES**

**1.0 OBJECTIVE**

The Federal Information Security Management Act (FISMA) of 2002 requires that each agency develop, document, and implement an agency wide information security program, approved by the Director under section 3543(a)(5), to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by (1) another agency, (2) contractor, or (3) other source, that includes – periodic assessments of the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency.

The purpose of this task order is to obtain professional services to support the Nuclear Regulatory Commission (NRC) in its annual information systems security self-assessment services (AISSS) consistent with National Institute of Standards and Technology (NIST) Draft NIST Special Publication 800-26 Revision 1 (including Appendix A System Questionnaire): Guide for Information Security Program Assessments and System Reporting Form and NIST Special Publication 800-53 Revision 1 including Appendix G. Specifically, the contractor shall assist NRC in completing the required security self assessments system questionnaires for all NRC Major Applications (MA), General Support Systems (GSS), and Contractor facilities using the System Questionnaire with NIST SP 800-53, "Recommended Security Controls for Federal Information Systems" References and Associated Security Control Mappings" Date April 2005 format.

**2.0 SCOPE OF WORK**

The Contractor shall provide all personnel, materials, hardware, software, labor, supplies, equipment, travel and other direct costs necessary to accomplish the performance of the activities described below. Last year self assessments will be used as the baselines and FY 2007 self assessments to be performed will be built on top of previous year work.

**Sponsor Office:** Office of information Services – Business Process Improvement and Application Development.

**System Owner:** Multiple Offices in NRC.

**System Description:** All major applications, general support systems, and contractor facilities in NRC are prioritized in the table follows:

**Status:** All systems and sites are in operation.

### 3.0 PERIOD OF PERFORMANCE

The period of performance of this task order is from June 1, 2007 until all of the Self Assessments are completed and signed by the system owners but the period of performance shall not exceed August 15<sup>th</sup>, 2007.

### 4.0 FUNDING

- (a) The total estimated amount (ceiling) for the products/services ordered, delivered, and accepted under this task order is **\$218,290.79**.
- (b) The amount presently obligated with respect to this task order is **\$214,604.00**. 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.

### 5.0 TRAVEL

Travel to the 4 NRC Regional locations and the Technical Training Center, Tennessee and the CNWRA facility in San Antonio, Texas. Travel to each location shall be for 2 days and 1 night, for one security analyst. All travel, other than local travel, requires the prior approval of the Project Officer.

### 6.0 SCHEDULE

The Contractor shall provide final System Questionnaire with NIST SP 800-53, "Recommended Security Controls for Federal Information System" (Self Assessments) reports for each system consistent with the NRC-approved integrated project plan (Subtask 1).

### 7.0 SPECIFIC TASKS

The Contractor shall be required to provide the following information security services in support of NRC AISSS. The Contractor shall perform, on all NRC Major Applications (MA), General support Systems (GSS), and NRC support contractor facilities (e.g. software development contractors, hardware support contractors, telecommunications, etc.) an inclusive, independent audit consistent with NIST Special Publication 800-26 Revision 1: (including Appendix A System Questionnaire): Guide for Information Security Program Assessments and System Reporting Form. The contractor shall use the following report format" System Questionnaire with NIST SP 800-53, "Recommended Security Controls for Federal Information Systems" References and Associated Security Control Mappings" Date April 2005. This audit shall include the review, verification and validation of all major and GSS systems documentation, analysis, penetration, vulnerability, configuration, system integrity, and patch management scans.

The Contractor shall identify, analyze, the currency of the systems security posture and ensures that controls are operating as intended relative to each control family identified in the NIST Special Publication 800-53 Revision 1: recommended Security Controls for Federal Information Systems. The contractor shall review NRC information systems security vulnerability trends at an agency and system level with special attention to those deficiencies that would impact NRC FISMA compliance.

## DR-33-06-317-T032

The contractor shall provide security analyst support to develop all requisite AISSS documentation such that all required Major Application, General Support Systems, and contract facilities AISSS reports have been completed and approved by the System owner.

### **Subtask 1: Integrated Security Activity Project Plan.**

Develop and implement a project plan to ensure completion of the annual information systems security self assessments 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 system or site level (i.e., each system or site for which an annual self assessment 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: Annual Analysis of Systems Documentation, Security Controls, Requirements, and Implementation Status, Report Generation, Review, Verification, and Validation of Self Assessment Report.**

The Contractor shall perform an independent audit and document self assessment reports that reviews 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 Rev 1 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 use the "System Questionnaire with NIST SP 800-53, "Recommended Security Controls for Federal Information Systems" References and Associated Security Control Mappings" Date April 2005 as the format for each self assessment.

Upon completion of the independent audit, the contractor shall complete the self-assessment document (System Questionnaire with NIST SP 800-53, "Recommended Security Controls for Federal Information Systems" References and Associated Security Control Mappings" Date April 2005) and coordinate with the NRC systems owners to verify that the information entered in the self-assessment is correct and accurate. The contractor shall document, in detail, the NRC system owner(s) rationale for each answer in the questionnaire. For example, why a security control is not being fully implemented (e.g. existence of compensating controls) or why it is overly rigorous would be addressed. All responses included in the self-assessment System Questionnaire shall fully convey to a user not familiar with the system or process, the rationale and requirements associated with each control. The responses shall also meet the requirements of each security control, address the level of effectiveness of security controls and documentation as described in draft Special

**DR-33-06-317-T032**

Publication (SP) 800-26 Revision 1. Guide for Information Security Program Assessments and System Reporting.

Upon verification and validation of the state of the systems security controls with the NRC system owner, the contractor and NRC system owner shall sign the security self-assessment systems questionnaire thereby affirming the accuracy and timeliness of the information provided.

All deliverables shall be delivered no later than August 15, 2007. Deliverables are to be transmitted with cover letter, on the contractor's letter head, describing the contents and identifying contract/order number and title.