ORDER FOR SUPPLIES OR SERVICES

PAGE OF PAGES: 1 | 1

IMPORTANT: Mark all packages and papers with contract and/or order numbers. BPA NO. DR-33-05-386

1. DATE OF ORDER: MAY 12 2006	2. CONTRACT NO. (If any): GS35F0229K
3. ORDER NO.: DR-33-05-386-T009 MODIFICATION NO	4. REQUISITION/REFERENCE NO: CIO-05-386-10

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-6F41
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 STE 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:
TRANSFER FUNDS FROM DR-33-05-386 TO DR-33-05-386-T009:
57N-15-5H2-357 N7235 252A 31X0200 $30,193.18

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			Net 30

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)
	The Contractor shall provide the U.S. Nuclear Regulatory Commission with "Security Categorization" support in accordance with the attached Performance Based Statement of Work, the terms and conditions of GSA Contract GS-35F-0229K, and the attached schedule.	[redacted]			$30,193.18	
	ATTACHMENTS: [redacted] 2. Statement of Work					
	ACCEPTANCE: [signature] 5/23/2006 SIGNATURE DATE Michael P. Norcio, Chairman and CEO PRINT NAME/TITLE					

SEE BILLING INSTRUCTIONS ON REVERSE

18. SHIPPING POINT | 19 GROSS SHIPPING WEIGHT | 20. INVOICE NO.

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: Eleni Jernell
c. CITY: Washington | d. STATE: DC | e. ZIP CODE: 20555

$30,193.18 — 17(h) TOTAL (Cont. pages)
$30,193.18 — 17(i). GRAND TOTAL

22. UNITED STATES OF AMERICA BY (Signature): [signature]

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

AUTHORIZED FOR LOCAL REPRODUCTION
PREVIOUS EDITION NOT USABLE

TEMPLATE - ADM001

SUNSI REVIEW COMPLETE

ADM002

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

PERFORMANCE BASED STATEMENT OF WORK
Task Order #9

PROJECT TITLE:	Security Categorization
NRC TECHNICAL ASSISTANCE:	Caroline Zabrucky
PROJECT MANAGER:	Carl Konzman
ALT PROJECT MANAGER:	Harry Kromer

1.0 Background

The purpose of this task order is to obtain Contractor professional services to assist the NRC in its information technology's security certification and accreditation process implementation. The Contractor will support NRC system owners with the development of security related documentation and systems analysis services required to obtain an authority to operate (i.e., operate the system in compliance with required standards) by providing a centralized security support services that will ensure cradle to grave compliance with FISMA, FEA, OMB M-04-04, NIST 800 Series, other applicable OMB and NIST series security certification and accreditation requirements.

2.0 Objective

The Contractor shall support the OIS in certification and accreditation of the Budget Formulation Application (BFA). The Contractor shall, at a minium, develop associated certification and accreditation documentation consistent with the security support tasks such that an authority to operate (ATO) which confers full accreditation shall be granted the system. The Contractor shall perform these security support tasks specified for LOW, MODERATE, and HIGH security baseline systems for each system category "Major", "General Support System", "Listed", and "Other."

3.0 Level of Effort

The estimated level of effort for this task is 1 FTE.

4.0 Period of Performance

The period of performance of this task order will start on May 15, 2006 through August 10, 2006.

5.0 Scope of Work

The Contractor shall provide security analyst staff to develop all requisite systems certification and accreditation documentation such that all systems obtain an Authority to Operate (ATO) no later than August 10, 2006.

The Contractor shall provide security analyst staff for the development of the associated documentation associated with the security support tasks specified below for a MODERATE Baseline system.

The Contractor shall support the NRC as follows:

Subtask 1:

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 hands-on system assessment
- 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
- 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 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 Security Test and Evaluation (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 Senior IT Security Officer must approve the final to enable system accreditation.

6.0 Meetings and Travel

Occasional travel to the NRC Headquarters offices located in Rockville, Maryland may be required. Local travel expenses will not be paid by the NRC. Parking on-site is not available.

7.0 NRC Furnished Material

NRC staff will provide copies of applicable NRC regulations, NRC Templates, and applicable guidance materials.

8.0 Contractor Acquired Material/Subcontractors

The Contractor shall obtain the necessary material and specialty subcontractors as necessary to perform the work under this effort.

9.0 Schedule

The Contractor shall provide final draft security documentation and reports for each system consistent with the Project Manager approved integrated project plan. NRC will provide security documentation templates and examples.

The Contractor shall provide final security documentation and reports for each system consistent with the Project Manager approved integrated project plan. NRC will provide security documentation templates and examples.

10.0 Deliverables

The Contractor shall provide:

Required Service	Service Type	Standard of Performance
22.14 Risk Assessment	Time and Materials	Critical
22.15 Systems Security Plan (SSP)	Time and Materials	Critical

Upon receipt of NRC comments on submitted draft reports, the contractor shall address each comment and revise the report as needed to address NRC input.

11.0 Technical Direction

Carl Konzman is designated as the OIS Technical Project Monitor (TPM) for this task. Harry Kromer is designated as the NRC Technical Assistance Project Manager (TAPM).

The OIS TPM is responsible for providing technical guidance to the performing organization regarding staff interpretations of technical aspects of regulatory requirements along with relevant documents when requested by the performing organization.

All work products must be reviewed and approved by the OIS TPM before they are submitted as final documents. All technical direction given to the performing organization must be consistent with the work scope and schedule.

The OIS TPM is not authorized to unilaterally make changes to the approved work scope or schedule or give the performing organization any direction that would increase costs over approved levels.

12.0 Performance Standards

Required Service	Service Type	Standard of Performance*	Method of Surveillance	Maximum Allowable Deviation from Standard Performance
22.14 Risk Assessment	Time and Materials	Critical	100% Inspection by Project Officer Customer Satisfaction Survey (Council Member Reviews/Project Sponsors)	0% deviation, looking for a minimum of 100% accuracy
22.15 Systems Security Plan (SSP)	Time and Materials	Critical	100% Inspection by Project Officer	0% deviation, looking for a minimum of 100% accuracy

NOTE: There shall be no cost corrective actions. Indefinite task/delivery orders will set forth the applicable standards.

*See contract for a description of performance standards.