Rcd: [illegible]

ORDER FOR SUPPLIES OR SERVICES

PAGE OF PAGES: 1 of 10

IMPORTANT: Mark all packages and papers with contract and/or order numbers. BPA NO. GS35F0229K

1. DATE OF ORDER: MAY 13 2009
2. CONTRACT NO. (If any):
3. ORDER NO.: DR-33-06-317-T059
MODIFICATION NO.:
4. REQUISITION/REFERENCE NO.: 33-06-317T059 DTD: 3/19/2009

5. ISSUING OFFICE (Address correspondence to):
U.S. Nuclear Regulatory Commission
Div. of Contracts
Attn: Michele D. Sharpe
Mail Stop: TWB-01-B10M
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: 2-C2M
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 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
97L-15-5I1-133 N7422 252A 31X0200.97L FFS# SEC09300
OBLIGATE $30,000; 910-15-5G1-348 J1243 252A 31X0200.910
FFS# 10970652C OBLIGATE $10,000

10. REQUISITIONING OFFICE: 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: Rockville, MD
b. ACCEPTANCE: Rockville, MD

14. GOVERNMENT B/L NO.:

15. DELIVER TO F.O.B. POINT ON OR BEFORE (Date):

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)
	The contractor shall provide the U.S. Nuclear Regulatory Commission (NRC) with, "Federal Information Security Management Act (FISMA) Continuous Monitoring Support" services in accordance the following: 1. Attached Statement of Work 2. Schedule of Supplies and Services and Price/Cost 3. Terms and Conditions of GSA Schedule No. GS35F0229K 4. Terms and Conditions of NRC Delivery Order No. DR-33-06-317 Reference: MAR Quotation (Ref# 2009-045/WA1435), dated 4/17/2009 ACCEPTANCE: Linda Klages 5/18/09 Signature Date Linda Klages, VP Contracts MAR, Incoporated Print Name/Title					

SEE BILLING INSTRUCTIONS ON REVERSE

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

21. MAIL INVOICE TO:
a. NAME: Department of Interior / NBC
NRCPayments@nbc.gov
b. STREET ADDRESS (or P.O. Box): Attn: Fiscal Services Branch - D2770
7301 W. Mansfield Avenue
c. CITY: Denver
d. STATE: CO
e. ZIP CODE: 80235-2230

17(h) TOTAL (Cont. pages): $126,746.04 (Base Yr)

17(i). GRAND TOTAL: $301,985.40(Base+Opt)

22. UNITED STATES OF AMERICA BY (Signature): Jordan Pulaski

23. NAME (Typed): Jordan Pulaski
TITLE: CONTRACTING/ORDERING OFFICER

AUTHORIZED FOR LOCAL REPRODUCTION
PREVIOUS EDITION NOT USABLE

SUNSI REVIEW COMPLETE MAY 21 2009

OPTIONAL FORM 347 (REV. 2/2001)
PRESCRIBED BY GSA/FAR (48 CFR) 53.213(f)

DELIVERY ORDER DR-33-06-317

TASK ORDER (59)

Federal Information Security Management Act (FISMA)

Continuous Monitoring Support

1.0 OBJECTIVE

The Contractor shall provide support to Nuclear Regulatory Commission (NRC) Program Offices for Federal Information Security Management Act (FISMA) Continuous Monitoring Support and to assist the offices in the development of their Information System Security Program (ISSP).

2.0 BACKGROUND

The offices listed in this task order will select from a menu of options specifying the tasks the contractor is to perform. Each column in the table will represent an individual office and funding will be specified by subtask so each office's expenditures can be tracked.

3.0 SCOPE OF WORK

The Contractor must ensure that the office's continuous monitoring efforts and ISSP meets all federally mandated and Nuclear Regulatory Commission (NRC) defined security requirements. The Contractor shall perform but will not be limited to the following:

- **Continuous Monitoring**

  The contractor shall support the organization in establishing and maintaining a Continuous Monitoring process that meets federally mandated and NRC defined security requirements.

  Coordinate Continuous Monitoring Efforts

  The Contractor shall assign a project manager to:

  - Coordinate the efforts described in this task order.
  - Serve as a point of contact between the organization and the Contractor.
  - Manage the task's triple constraints, which are cost, time, and scope.
  - Apply knowledge, skills, tools, and techniques to task order activities to meet or exceed expectations.
  - Work with the organization to ensure risks to their systems are minimized.
  - Assist the organization in establishing their continuous monitoring schedules so federally mandated and NRC defined security requirements are met.
  - Report any circumstances that might impact the ability of the contractor to meet the stated objectives of this task order to the NRC Project Officer and the organization's representative.
  - As needed, develop an agenda for status meetings and deliver that agenda to the NRC Project Officer and organization's representative 24 hours before the start of the meeting.

Quarterly Scanning

The Contractor shall conduct quarterly vulnerability scanning of the organization's systems. Quarterly scanning shall establish if the system's security controls are operating as intended and ensure systems continually meet federally mandated and NRC defined security requirements. All risks / deficiencies shall be measured according to NIST SP 800-30 "Risk Management Guide for Information Technology Systems".

The contractor shall use a variety of testing tools (Nessus, Core Impact, DISA Gold, Air Magnet, etc.), manual and automatic, including proprietary and modified open source, to conduct the assessment. All hardware and software used to support this task order must be approved by the NRC Project Officer.

Scanning shall consist of the following phases:

- Phase 1: Preparation – The contractor shall ensure all testing devices that are going to be used during the assessment are loaded with the latest patches, security updates, device drivers, and plug-ins.
- Phase 2: Information Gathering – The contractor shall conduct scans, review documentation, and interview personnel to gather the needed information to perform a risk analysis of the organization's systems.
- Phase 3: Draft Assessment Reports - The contractor shall develop System Assessment Reports that identify the risks each system poses to itself, its data, and the NRC infrastructure.
- Phase 4: Validate Findings – The contractor shall work with the System Owner, ISSOs and System Administrators to validate the findings, ensure risks have been properly assessed, and to develop mitigation strategies that will resolve the deficiencies.
- Phase 5: Finalize Assessment Reports – The contractor shall incorporate NRC's comments into the Assessment Reports and deliver the final version of the Assessment Reports to the NRC Project Officer.
- Phase 6: Plan of Action and Milestone (POA&M) Reports – The contractor shall incorporate any findings into each system's POA&M Report

The Assessment Reports and Updated POA&M Reports shall be submitted to NRC Project Officer for review and comment. All reports must be approved by the NRC Project Officer, the system owner, and ISSO. The Contractor shall revise and update each deliverable as appropriate and provide final versions to the NRC.

The contractor's Assessment Strategy shall include but will not be limited to the following:

- Identifying if the system is vulnerable to any published exploits
- Determining if the system has the latest patches installed
- Determining if the system is utilizing any unsupported hardware/software
- Analyzing if unnecessary ports or services are available
- Ensuring the system adheres to Federal regulations, guidelines, and standards
- Ensuring the system adheres to NRC hardening requirements
- Identifying if SANS top twenty or vendor identified vulnerabilities are present in the system
- Analyzing if the system's implementation adheres to the vendor's recommendations
- Ensuring the system's procedural controls are adequate
- Determining if the system's managerial controls are sufficient
- Analyzing weaknesses in the system's physical security

- Observing NRC employees, contractors, and vendors adherence to policy and procedures

Upon completion, the Contractor shall upload the test results and any resultant POA&M action items into the CSO FISMA tracking tool.

Conduct Vulnerability Assessments (as needed)

As needed, the Contractor shall conduct vulnerability assessments of the organization's systems. Vulnerability assessments shall establish if the system's security controls are operating as intended and ensure systems continually meet federally mandated and NRC defined security requirements. All risks and deficiencies shall be measured according to NIST SP 800-30 "Risk Management Guide for Information Technology Systems".

Vulnerability Assessments will follow the same methodology described under Quarterly Scanning.

Annual Controls Testing

The Contractor shall conduct annual control testing of the organization's information systems according to NIST SP 800-53A "Guide for Assessing the Security Controls in Federal Information Systems". The Contractor shall develop selection criteria to determine which security controls shall be tested. At a minimum, the selection criteria shall be based upon: the sensitivity level of the system; the requirement to annually test volatile controls; controls called out for annual testing in OMB guidance; CSO specified controls; and those associated with each system's POA&M items. This assessment shall be performed on all Major Applications and General Support Systems each fiscal year. Additionally, some Listed Systems may require testing.

The Contractor shall perform a comprehensive assessment of the selected management, operational, and technical security controls for each system. The assessment shall determine the extent to which each system's controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting federally mandated and NRC defined security requirements. Upon completion of testing the Contractor shall develop Annual Security Control Test Report for each system and incorporate any findings into each system's POA&M Report.

The draft Annual Security Control Test Reports and the POA&M Reports shall be submitted to NRC Project Officer, system owner, and ISSO for review and comment. The Contractor shall revise and update each deliverable as appropriate and provide final versions.

Upon completion, the Contractor shall upload the Annual Controls Testing results and any resultant POA&M action items into the CSO control tracking tool.

Update Certification and Accreditation Documentation

Annually, the Contractor shall update the C&A Package of all Major Applications and General Support Systems. The draft documents shall be submitted to organization for review and comment. The Contractor shall revise and update each deliverable as appropriate and provide final versions to NRC Project Officer, system owner, and ISSO.

This activity should be done in conjunction with the Annual Assessment.

Assist in Plan of Action and Milestone (POA&M) Reporting

Utilizing the NRC POA&M process, the Contractor shall update the POA&M Reports of all Major Applications and General Support Systems quarterly.

The Contractor shall collect information so the POA&Ms can be updated to reflect the current situation. Any new vulnerability that is discovered shall be added and assigned to the appropriate system. All

POA&M Reports shall be submitted for review and comment. The Contractor shall revise and update each deliverable as appropriate and provide final versions to the NRC Project Officer, system owner, and the ISSO.

Upon completion, the Contractor shall upload the POA&M Reports into the CSO control tracking tool.

- **Contingency Planning**

The contractor shall support the organization in establishing and maintaining a Contingency Planning process that meets federally mandated and NRC defined security requirements.

Contingency Plan

The Contractor shall support the NRC staff in the development and documentation of a Contingency Plan (CP) and test procedures. The System CP shall be documented in a report that follows the NRC Template for the System CP. The Plan shall be maintained in its hard copy form for contingency execution should the 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 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 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.

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. 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.

The Contingency Plan and Contingency Test & Report must be updated annually. The Contractor shall ensure that the steps, templates, and reports outlining the organization's Contingency Planning process follow NRC's Project Management Methodology.

- **ISSP Support**

The contractor shall support the organization in establishing and maintaining an ISSP that meets federally mandated and NRC defined security requirements.

Security Program Communications Support

The Contractor shall provide communications support when communicating with upper management, CSO staff, Office of Inspector General, or other responsible parties. Also, the Contractor will assist with the office's system specific and role based training.

Security Program Security Engineering Support

The Contractor shall provide Security Engineering support to verify and validate architectures and implementations are based on sound security engineering principles and practices. The Contractor shall ensure that all federally mandated and NRC defined security requirements are met.

Please note that any Contractor personnel working under this task order can not take on the role of certification agent for any of the systems defined in this statement of work. At no time is the Contractor allowed to configure an operational system.

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 (C&A) PROCESS AND DELIVERABLES".

4.0 TASKS

The Contractor shall support the program offices according to Consolidated Information Security Support Services (CISSS) 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: Office of Information Services (OIS) / Information and Records Services Division (IRSD)

As specified in the table below, the contractor will provide the following services to OIS/IRSD.

Agencywide Documents Access and Management System (ADAMS)

Type: Major Application

Sensitivity: High Confidentiality, High Integrity, and High Availability

Description: ADAMS supports document capture, distribution and dissemination, records management, and search and retrieval by both NRC staff and the public. ADAMS stores and processes information that is designated sensitive unclassified information or below, that consists of programmatic and administrative materials generated both internally and externally in various formats and are made available to the Government or the public for reference and reuse.

Subtask 3: Office of the Secretary (SECY)

As specified in the table below, the contractor will provide the following services to SECY.

EHD

Electronic Hearing Docket (EHD)

Type: Major Application

Sensitivity: Moderate Confidentiality, Moderate Integrity, and Moderate Availability

Description: EHD is a major application that supports the confidentiality, integrity, and availability (CIA) of hearing documents electronically. The EHD includes the Protected Order File (POF) component that controls restrictive access to information. Together, the EHD domain and POF domain process and control collections

of documents pertinent to the adjudicatory proceedings in order to make them available to concerned parties and the public.

Tasks	Sub Task 2 OIS/IRD		Sub Task 3 SECY	
Automated Information Systems	**ADAMS**		**EHD**	
	Base	**Option Year 1**	**Base**	**Option Year 1**
Continuous Monitoring: Coordinated Monitoring Efforts	NA	NA	Shall develop and update Qtrly a schedule of events for continuous monitoring efforts	Shall develop and update Qtrly a schedule of events for continuous monitoring efforts
Continuous Monitoring: Quarterly Scanning	NA	Shall perform Qtrly Scanning	Shall perform Qtrly Scanning	Shall perform Qtrly Scanning
Continuous Monitoring: Vulnerability Assessments	NA	NA	NA	NA
Continuous Monitoring: Annual Controls Testing	NA	Shall perform annual controls testing during the 3rd Qtr	NA	Shall perform annual controls testing during the 3rd Qtr
Continuous Monitoring: Update Certification and Accreditation Documentation	Shall annually update ATO package	Shall annually update ATO package	Shall annually update ATO package	Shall annually update ATO package
Continuous Monitoring: POA&M Reporting	NA	NA	NA	NA
Contingency Plan	Shall update contingency plan	Shall update contingency plan	Shall update contingency plan	Shall update contingency plan
Contingency Test and Test Report	Shall update contingency test and test report	Shall update contingency test and test report	Shall update contingency test and test report	Shall update contingency test and test report
ISSP Support: Communications Support	NA	NA	Shall provide communications support for continuous monitoring efforts	Shall provide communications support for continuous monitoring efforts
ISSP Support: Security Engineering Support	NA	NA	Shall provide security engineering support for continuous monitoring efforts	Shall provide security engineering support for continuous monitoring efforts

5.0 PERIOD OF PERFORMANCE

The period of performance for this task order is date of award plus one year with one (1) one-year option. The exercise of Option Year 1 under the task order is only applicable if the option year of the base contract (DR-33-06-317) is exercised.

6.0 FUNDING

(a) The total estimated amount (ceiling) for the products/services ordered, delivered, and accepted under this task order is **$126,746.04**.

(b) The amount presently obligated with respect to this task order is **$40,000.00**. 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 is done so at the Contractor's sole risk.

6.0 TRAVEL

Travel is not expected for this task order.

7.0 MEETINGS

The Contractor's Project Manager and technical lead shall attend monthly status meetings at NRC Headquarters with the NRC Project Officer and/or organizational representatives. This meeting will be used to discuss work being done under this task order and any issues that may have arisen during the last week.

Additionally, the contractor will attend scheduled quarterly compliance review meetings at the start of each quarter. These meetings will be chaired by the Chief Information Security Officer (CISO).

OTHER TERMS AND CONDITIONS

A.1 52.217-8 OPTION TO EXTEND SERVICES (NOV 1999)

The Government may require continued performance of any services within the limits and at the rates specified in the contract. These rates may be adjusted only as a result of revisions to prevailing labor rates provided by the Secretary of Labor. The option provision may be exercised more than once, but the total extension of performance hereunder shall not exceed 6 months. The Contracting Officer may exercise the option by written notice to the Contractor within 60 days of the expiration of the task order.

A.2 52.217-9 OPTION TO EXTEND THE TERM OF THE CONTRACT (MAR 2000)

(a) The Government may extend the term of this contract by written notice to the Contractor within 30 days; provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least 60 days before the contract expires. The preliminary notice does not commit the Government to an extension.

(b) If the Government exercises this option, the extended contract shall be considered to include this option clause.

(c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed two years.

A.3 ANNUAL AND FINAL CONTRACTOR PERFORMANCE EVALUATIONS

Annual and final evaluations of contractor performance under this task order will be prepared in accordance with FAR 42.15, "Contractor Performance Information," normally at the time the contractor is notified of the NRC's intent to exercise the task order option. If the multi-year task order does not have option years, then an annual evaluation will be prepared (state time for annual evaluation). Final evaluations of contractor performance will be prepared at the expiration of the task order during the closeout process.

The Contracting Officer will transmit the NRC Project Officer's annual and final contractor performance evaluations to the contractor's Project Manager, unless otherwise instructed by the contractor. The contractor will be permitted thirty days to review the document. The contractor may concur without comment, submit additional information, or request a meeting to discuss the performance evaluation. The Contracting Officer may request the contractor's Project Manger to attend a meeting to discuss the performance evaluation.

Where a contractor concurs with, or takes no exception to an annual performance evaluation, the Contracting Officer will consider such evaluation final and releasable for source selection purposes. Disagreements between the parties regarding a performance evaluation will be referred to an individual one level above the Contracting Officer, whose decision will be final.

The Contracting Officer will send a copy of the completed evaluation report, marked "For Official Use Only," to the contractor's Project Manager for their records as soon as practicable after it has been finalized. The completed evaluation report also will be used as a tool to improve communications between the NRC and the contractor and to improve task order performance.

The completed annual performance evaluation will be used to support future award decisions in accordance with FAR 42.1502(a) and 42.1503(c). During the period the information is being used to provide source selection information, the completed annual performance evaluation will be released to only two parties - the Federal government personnel performing the source selection evaluation and the contractor under evaluation if the contractor does not have a copy of the report already.