

ORDER FOR SUPPLIES OR SERVICES

PAGE OF PAGES

1 10

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

BPA NO.

1. DATE OF ORDER MAR 06 2009	2. CONTRACT NO. (if any) GS-35F-0229K	6. SHIP TO:	
3. ORDER NO. DR-33-06-317-T055	MODIFICATION 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: Michele D. Sharpe Mail Stop: TWB-01-B10M Washington, DC 20555		b. STREET ADDRESS Attn: Bill Dabbs 11545 Rockville Pike Mail Stop: T-2-C-2	
7. TO:		c. CITY Washington	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 STE 204	<input type="checkbox"/> a. PURCHASE	<input checked="" type="checkbox"/> b. DELIVERY
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.	
e. STATE MD	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.	
f. ZIP CODE 208506106	10. REQUISITIONING OFFICE CIO CSO	
9. ACCOUNTING AND APPROPRIATION DATA B&R: 910-15-5E1-334 JC: J1048 BOC: 252A APPN No.: 31X0200.90 DUNS#: 062021639	\$40,000.00	

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)	16. DISCOUNT TERMS
a. INSPECTION Rockville, MD	b. ACCEPTANCE Rockville, MD			

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 55 UNDER NRC ORDER DR-33-06-317 (CISSS): The contractor shall provide the U.S. Nuclear Regulatory Commission (NRC) with, "Infrastructure Computer Operations Division (ICOD) Continuous Monitoring" services in accordance with the following:</p> <ul style="list-style-type: none"> - The attached Statement of Work (SOW) - The attached Schedule of Supplies or Services and/or Price - The terms and conditions of GSA Schedule GS-35F-0229K - The terms and conditions of NRC Order No. DR-33-06-317 <p>Reference: MAR Quotation (Ref #2009-012/WA138), dtd 2/13/2009.</p> <p>ACCEPTED:</p> <p><i>Linda Klages</i> 3/13/09 Signature Date</p> <p><u>Linda Klages, VP Contracts, MAR INC</u> Print/Name and Title</p>					

SEE BILLING INSTRUCTIONS ON REVERSE	18. SHIPPING POINT	19. GROSS SHIPPING WEIGHT	20. INVOICE NO.	\$622,061.61	17(h) TOTAL (Cont. pages)
	21. MAIL INVOICE TO:				
	a. NAME Department of Interior / NBC NRCPayments@nbc.gov			\$1,114,953.12	17(i). GRAND TOTAL
	b. STREET ADDRESS (or P.O. Box) Attn: Fiscal Services Branch - D2770 7301 W. Mansfield Avenue	c. CITY Denver	e. ZIP CODE 80235-2230		

22. UNITED STATES OF AMERICA BY (Signature) <i>Lew Larnall</i>	23. NAME (Typed) Eleni Jernell Contracting Officer TITLE: CONTRACTING/ORDERING OFFICER
--	---

AUTHORIZED FOR LOCAL REPRODUCTION
PREVIOUS EDITIONS OBSOLETE

SUNSI REVIEW COMPLETE

MAR 19 2009

OPTIONAL FORM 347 (REV. 02/2006)
PRESCRIBED BY GSA FPMR (41 CFR) 101-11.6

DMDC

DELIVERY ORDER DR-33-06-317
TASK ORDER (55)
Office of Information Services (OIS)
Infrastructure Computer Operations Division (ICOD)
Continuous Monitoring

1.0 OBJECTIVE

The Contractor shall support the Office of Information Services (OIS) Infrastructure Computer Operations Division (ICOD) Information System Security Program (ISSP).

2.0 BACKGROUND

This task order will provide contractor support for the following OIS/ICOD systems:

- Information Technology Infrastructure (ITI) – General Support System
- Telecommunication Services (Telecomm) – General Support System
- Electronic Mail Systems (E-MAIL) – Major Application
- Managed Public Key Infrastructure (MPKI) – General Support System

Note: The security categorization document for each system will specify the system's sensitivity (High, Moderate, and Low).

3.0 SCOPE OF WORK

The Contractor must ensure the OIS / ICOD ISSP meets all federally mandated and Nuclear Regulatory Commission (NRC) defined security requirements. The Contractor shall perform the following: Integrated Security Activity Planning & Scheduling; Continuous Monitoring; Security Engineering; and Support Services.

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 OIS/ICOD ISSP according to Consolidated Information Security Support Services (CISSS) SOW Enclosure 6 and Section B "Schedule of Supplies or Services and Prices".

Please note that any Contractor personnel working under this task order can not take on the role of certification agent for any OIS/ICOD system. "Certification Agent" is defined as an individual, group, or organization responsible for conducting a security certification, or comprehensive assessment of the management, operational, and technical security controls in an information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. The certification agent also provides recommended corrective actions to reduce or eliminate vulnerabilities in the information system. Prior to initiating the security assessment activities that are a part of the certification process, the certification agent

provides an independent assessment of the system security plan to ensure the plan provides a set of security controls for the information system that is adequate to meet all applicable security requirements.”

At no time is the Contractor allowed to configure an OIS/ICOD operational system.

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 occur 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.

Note: All parties working under this task order will contribute to the development and maintenance of the integrated schedule.

Subtask 2: Continuous Monitoring

This subtask contains the following elements:

2.1: 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 OIS/ICOD & 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 OIS/ICOD expectations.
- Work with OIS/ICOD to ensure risks to their operational systems are minimized.
- Assist OIS/ICOD in establishing their continuous monitoring schedules so federally mandated and NRC defined security requirements are met.
- Report at the weekly meeting all circumstances that impact the ability of the contractor to meet the stated objectives of this task order to the NRC Project Officer and OIS/ICOD representative.

- Develop an agenda for the weekly status meeting and deliver that agenda to the NRC Project Officer and OIS/ICOD representative by close of business each Monday.

2.2: Adhoc Vulnerability Assessments

The Contractor shall conduct vulnerability assessments of OIS/ICOD systems as needed.

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 / deficiencies shall be measured according to NIST SP 800-30 "Risk Management Guide for Information Technology Systems".

Tools

The contractor shall use a variety of testing tools (Nessus, Core Impact, DISA Gold, Air Magnet, Hailstorm, 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.

Process

This Vulnerability Assessment shall contain 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 OIS/ICOD 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 deliverable the final version of the Assessment Reports to the NRC Project Officer.
- Phase 6: Summary Assessment Report – The contractor shall develop a Summary Assessment Report aggregating the findings across all OIS/ICOD systems. The Summary Report shall document the overall risk the organization has incurred as well as any observed vulnerability trends.
- Phase 7: Plan of Action and Milestone (POA&M) Reports – The contractor shall incorporate any findings into each system's POA&M Report

The Assessment Reports, Summary Assessment Report, 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, OIS/ICOD System Owner, and OIS/ICOD ISSOs. The Contractor shall revise and update each deliverable as appropriate and provide final versions to the NRC.

The contractor's Vulnerability 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.

2.3: Annual Assessment

The Contractor shall conduct an annual assessment of ICOD'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 OIS/ICOD Major Applications and General Support Systems during the 3rd quarter of each fiscal year.

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. for each system consistent with NIST SP 800-53A.

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 OIS/ICOD for review and comment. The Contractor shall revise and update each deliverable as appropriate and provide final versions to OIS/ICOD.

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

The annual assessment shall be done once a year.

2.4: Update System Documentation

The Contractor shall update the C&A Package of all OIS/ICOD Major Applications and General Support Systems.

The draft documents shall be submitted to OIS/ICOD for review and comment. The Contractor shall revise and update each deliverable as appropriate and provide final versions to OIS/ICOD.

This activity must be done in conjunction with the Annual Assessment. The update of OIS/ICOD system documentation shall occur annually.

Subtask 3: Security Engineering

This subtask contains the following elements:

3.1: Security Program Communications Support

The Contractor shall provide communications support when OIS/ICOD is communicating with upper management, CSO staff, Office of Inspector General, or other responsible parties.

3.2: Supporting Documentation

The Contractor shall develop documentation that identifies how the system's security controls have been implemented. Documentation will include details about the system's technical, managerial, and procedural controls.

3.3: Security Engineering Services

The Contractor shall provide Security Engineering Services to verify and validate the OIS/ICOD proposed system architectures and implementations are based on sound security engineering principles and practices. In addition, the Contractor shall ensure that all federally mandated and NRC defined security requirements are met.

Subtask 4: Support Services

This subtask contains the following elements:

4.1: Review and Update OIS/ICOD Management Directives

The Contractor shall review and update the management directive(s) (MD) and their respective handbook(s) listed in the table below. The Contractor shall ensure that all updates reflect current trends and technologies. The Contractor shall leverage industry leading practices, Federal mandates and guidance (including Presidential Directives, Homeland Security Directives, and National Communications System directives), existing NRC documentation, feedback from ICOD staff, and other relevant sources. The contractor shall ensure the management directive(s) and their respective handbooks fully address federally mandated and NRC defined security requirements. All updates shall be made by the completion date identified in the table below.

MD #	MD Description	Point of Contact	Completion Date
------	----------------	------------------	-----------------

2.3	Telecommunications	Primary: Robert Miller Secondary: Stanley Wood	March 31, 2009
-----	--------------------	---	----------------

Effective management directives and associated handbooks will be:

- Concise and to the point
- Developed to meet a business need or compliance requirement or address a realistic risk
- Compatible with the organization culture and likely to be widely accepted
- Reasonable
- Enforceable
- Auditable
- Well communicated
- Capable of being used to assess or measure security
- Supported by management
- Kept up to date and reviewed annually

The following deliverables will be developed under this subtask:

- Management Directive Format (the directive's outline)
- Handbook Format (the handbook's outline)
- Management Directive
- Associated Handbook
- Engineering notebook containing all supporting documentation and notes that details why decisions were made.

4.2: Configuration Management

The contractor shall analyze the effectiveness of ICOD's current configuration management mechanisms, and develop a configuration management approach which addresses identified deficiencies. The contractor shall leverage NIST 800-53 (Recommended Security Controls for Federal Information Systems) to develop the plan. The contractor will assist ICOD with executing the plan.

The following deliverables will be developed under this subtask:

- Gap Analysis Report- Identifies the differences between what has been implemented and what is required for implementing a configuration management process that fully addresses federally mandated and NRC defined requirements.
- Configuration Management Plan – Identifies the organization's configuration management process and contains appendices that specify the configuration items of each system defined in this task order.
- Configuration Management Implementation Plan - Specifies how the new configuration management process will be stood up.

- Audit/Status Accounting Implementation Plan – Identify processes, procedures, and tools that can be used to ensure systems are being properly controlled using the new configuration management process.
- Training Plan – Specifies how the staff will be trained to utilize the new configuration management process.

4.3: Disaster Recovery

Develop a process and procedures to adequately address emergency preparedness and continuity of operations associated with NRC's infrastructure systems. The contractor shall work with ICOD to perform a business impact analysis in accordance with NIST 800-34 (Contingency Planning Guide for Information Technology Systems). The contractor shall use this analysis to evaluate alternatives against several criteria to identify gaps between the current levels of redundancy and the levels required by the organization. The contractor shall assist ICOD with documenting the Disaster Recovery (DR) Plan that addresses the people, processes, and systems necessary to successfully fail-over the systems, and provide ongoing support as needed. The contractor shall ensure that the DR plan and related deliverables are in compliance with NCS 2.10, all Federal mandated policies/directives, and NRC defined requirements. The contractor shall assist ICOD with developing alternative site criteria and selection. The contractor shall assist ICOD with the implementation and testing of the DR plan. The contractor shall provide ICOD with additional support in the DR area, as requested.

The following deliverables will be developed under this subtask:

- Impact Analysis – Identifies and analyze the impact various disaster scenarios would have on the systems defined in this task order. Also, the Impact Analysis will identify if a system's disaster recovery process has undergone a significant change that requires an immediate update of the system's contingency plan.
- Inventory – Collect information about the organization's systems (hardware and software components) and develop an inventory of the skills possessed by ICOD's staff and contractors.
- Gap Analysis - Identify gaps between the current state of readiness and the capabilities required to satisfy the federally mandated and NRC defined recovery requirements.
- Alternatives Matrix - Each alternative should be evaluated using cost, probability, and impact to determine the best solution for the organization. The alternatives will represent a realistic approach that can be implemented within the agency.
- Contingency Plan/Disaster Recovery Plan - Document the people, processes, hardware, and software to successfully fail-over the systems defined in this task order.
- Supporting Documentation - Training, maintenance, and testing plans required to sustain the developed strategy.

Instructions for Deliverables

Deliverables shall be consistent with this statement of work. If for any reason a deliverable cannot be delivered within the specified time frame, the contractor shall notify the NRC Project Officer in writing with cause and the proposed revised time frame. This notice shall include the impact on the overall project. The NRC Project Officer shall make a business decision about the impact of the delay and forward the impact to the Contracting Officer.

Each deliverable shall first be submitted in draft for NRC review. NRC shall have 10 business days to review each draft deliverable and respond with comments or approval. If more time is required, the contractor will be notified in writing by the NRC Project Officer.

If revisions are required, the contractor has 5 business days to complete the revisions and submit the revised draft deliverable to the NRC Project Officer. Once the deliverable is approved by NRC Project Officer, the deliverable will become final. For each deliverable (draft or final), the contractor shall provide one (1) hardcopy and one (1) electronic version of the deliverable to the NRC Project Officer, unless otherwise indicated. All written deliverables shall be phrased in language that can be understood by the non-technical layperson. Statistical and other technical terms used in the deliverable shall be defined in a glossary.

All deliverables developed under this task order must be formatted in Microsoft Word (version 2003 or later version as approved by the Project Officer). All deliverables and supporting documentation gathered or developed under this task order may not be stored on any device or piece of equipment that has not been approved by the NRC Project Officer.

5.0 PERIOD OF PERFORMANCE

The period of performance for this task order is date of award plus one year with one 1-year option.

6.0 FUNDING

- (a) The total estimated amount (ceiling) for the products/services ordered, delivered, and accepted under this task order is **\$622,061.61** (includes **\$20,000** for NTE travel).
- (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.

7.0 TRAVEL

Travel for the task order should not exceed **\$20,000.00** per year.

8.0 MEETINGS

The contractor's technical representative shall attend bi-monthly status meetings at NRC Headquarters on the first and fifteenth of each month. During these meetings the Contractor and the NRC will discuss ongoing work, issues, and upcoming work that needs to be done. Contractor will propose an agenda for the meeting and will send the agenda to the NRC Project Officer 2 business days before the meetings are to be held. The NRC Project Officer will finalize the agenda and distribute the agenda the day before the meeting.

TASK ORDER TERMS AND CONDITIONS

A.1 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 calendar days; provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least 60 calendar 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.2 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 task order. 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 1 year. The Contracting Officer may exercise the option by written notice to the Contractor within 60 days of the expiration of task order.