

ORDER FOR SUPPLIES OR SERVICES

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

BPA NO. GS35F0229K

1. DATE OF ORDER APR 30 2009		2. CONTRACT NO. (If any) GS35F0229K		6. SHIP TO:			
3. ORDER NO. DR-33-06-317-T057		4. REQUISITION/REFERENCE NO. 33-06-317T057 FFS# CSO09310		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: 2-C2M		c. CITY Washington	
				d. STATE DC		e. ZIP CODE 20555	
7. TO:				f. SHIP VIA			
a. NAME OF CONTRACTOR MAR, INCORPORATED				8. TYPE OF ORDER			
b. COMPANY NAME				<input type="checkbox"/> a. PURCHASE		<input checked="" type="checkbox"/> b. DELIVERY	
c. STREET ADDRESS 1803 RESEARCH BLVD STE 204				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.		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.	
d. CITY ROCKVILLE		e. STATE MD	f. ZIP CODE 208506106				
9. ACCOUNTING AND APPROPRIATION DATA B&R: 97S-15-5D1-328 JC: N7343 BOC: 252A APPN No.: 31X0200 FFS#: CSO09310 DUNS#: 062021639				10. REQUISITIONING OFFICE CSO			
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 SMALL BUSINESS			
13. PLACE OF		14. GOVERNMENT B/L NO.		15. DELIVER TO F.O.B. POINT ON OR BEFORE (Date)		16. DISCOUNT TERMS NET 30	
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>The contractor shall provide the U.S. Nuclear Regulatory Commission (NRC) with, "Computer Security Office (CSO) Certification & Accreditation" services in accordance with the following:</p> <ol style="list-style-type: none"> Attached Statement of Work Schedule of Supplies or Services and Price/Cost Terms and Conditions of GSA Schedule No. GS35F0229K Terms and Conditions of NRC Delivery Order No. DR-33-06-317 <p>Reference: MAR Quotation (Ref# 2009-031/WA1415), dated 3/17/2009</p> <p>ACCEPTANCE:</p> <p><i>Linda Klages</i> Signature _____ Date <u>4/22/09</u></p> <p><u>Linda Klages, VP Contracts, MAR Incorporated</u> Print Name/Title</p>					

18. SHIPPING POINT		19. GROSS SHIPPING WEIGHT		20. INVOICE NO.		17(h) TOTAL (Cont. pages)
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						17(i). GRAND TOTAL
c. CITY Denver		d. STATE CO	e. ZIP CODE 80235-2230	\$120,068.01 (CEILING)		
SEE BILLING INSTRUCTIONS ON REVERSE						

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

AUTHORIZED FOR LOCAL REPRODUCTION
UNLESS INDICATED OTHERWISE
TEMPLATE - APPROOT

SUNSI REVIEW COMPLETE AUG 28 2009

ADM002

DELIVERY ORDER DR-33-06-317

TASK ORDER (57)

Computer Security Office (CSO) Certification and Accreditation Support

1.0 OBJECTIVE

The contractor shall support the Computer Security Office (CSO) in the certification and accreditation of the following:

- Information Assurance System (IAS) – Major Application
Sensitivity: Confidentiality H, Integrity H, and Availability M

2.0 BACKGROUND

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

IAS

The IAS system consists of several Commercial Off the Shelf (COTS) products loaded, tested and operated on a separate subnet that is capable of accessing the entire NRC network. The COTS products to be installed on hardened servers include but are not limited to: Encase, Hailstorm, Threatguard, and Secure Elements.

Each of these products provides a necessary automated IT Security capability for the CSO. The greatest benefit of having this suite of tools is that it will provide a real-time situational awareness capability to the members of the CSO Cyber Security Awareness (CSA) Team. Rather than relying on other NRC organizations to provide filtered information to the CSO/CSA, the combination of these capabilities will enhance the mission of the CSA and allow it to perform its essential duties autonomously. The implementation of this capability will provide the platform to receive critical Cyber security information first hand and unfiltered.

This system is presently in development.

3.0 SCOPE OF WORK

The contractor must ensure the system has been installed, configured, and maintained according to federally mandated and Nuclear Regulatory Commission (NRC) defined security requirements. The contractor will identify any operational risks found that may affect the system's ability to perform its mission and protect its data (stored and transmitted). The contractor shall perform the following:

<u>Tasks</u>	<u>IAS</u>
Subtask 2 - E-Authentication Risk Assessment	N/A

Tasks	IAS
Subtask 3 - Security Categorization Package <ul style="list-style-type: none"> • Security Categorization Document • Security Categorization Memo • Privacy Impact Assessment • Records Management Form 637 	N/A
Subtask 4 - Security Risk Assessment (SRA)	Shall develop the SRA.
Subtask 5 - System Security Plan (SSP)	Shall develop the SSP.
Subtask 6 - Preliminary System Testing	NA.
Subtask 7 - Standard Test and Evaluation (ST&E) Plan	Shall develop ST&E Plan
Subtask 8 - System Testing <ul style="list-style-type: none"> • ST&E Report • Vulnerability Assessment Report • Corrective Action Plan 	Shall perform system testing
Subtask 9 - Authority To Operate (ATO) Package <ul style="list-style-type: none"> • Approval to Operate Memo • Package Includes Named Deliverables 	Shall put together an ATO Package for system owner The ATO package is due to the system owner: 7/1/2009.

The contractor shall ensure that the steps, templates, and reports outlining certification and accreditation 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 SOW ENCLOSURE 6 of Delivery Order DR-33-06-317 "C&A PROCESS AND DELIVERABLES" for unclassified systems.

4.0 FUNDING

- (a) The total estimated amount (ceiling) for the products/services ordered, delivered, and accepted under this task order is **\$120,068.01**.
- (b) The amount presently obligated with respect to this task order is **\$60,000**. 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 PERIOD OF PERFORMANCE

The period of performance of this task order is one year from date of award.

6.0 SCHEDULE

The contractor shall provide 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 Certification and Accreditation effort according to 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: E-Authentication Risk Assessment

The contractor shall perform this task as identified in the table found in section 3 "Scope of Work".

Electronic authentication (e-authentication) is the process of establishing confidence in user identities electronically presented to an information system. The focus is on remote authentication of individual people over a network, for the purpose of electronic government or commerce. The OMB M-04-04 memorandum guidance applies to systems that have remote authentication of users of Federal agency information

technology systems for the purposes of conducting Government business electronically (or e-government). The guidance does not apply to internal only systems or the authentication of servers, or other machines and network devices. NRC's policy is to only require separate E-authentication Risk Assessments on systems where it is required. E-Authentication Risk Assessments shall be consistent with OMB M04-04, NIST SP 800-30, NIST SP 800-60A, and NIST SP 800-63.

Subtask 3: Security Categorization Package

The contractor shall perform this task as identified in the table found in section 3 "Scope of Work".

Security categorization standards for information and information systems provide a common framework and understanding for expressing security that, for the federal government, promotes: (i) effective management and oversight of information security programs; (ii) consistent reporting to the Office of Management and Budget (OMB) and Congress on the adequacy and effectiveness of information security policies, procedures, and practices. NRC's Security Categorization Package contains the following deliverables: Security Categorization Memo, Security Categorization Document, Privacy Impact Assessment, and Records Management Form 637.

A Security Categorization Package shall be completed for each new major application/general support system, listed system, contractor system, and those owned by other Federal agencies.

Subtask 4: Security Risk Assessment

The contractor shall perform this task as identified in the table found in section 3 "Scope of Work".

This Assessment is an important activity in an agency's information security program that directly supports security accreditation and is required by the FISMA and OMB Circular A-130, Appendix III. This assessment influences the development of the security controls for an information system and generates much of the information needed for the system's security plan.

The assessment shall characterize the information processed by using FIPS 199, Standards for Security Categorization of Federal Information and Information Systems and NIST 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 system configuration assessments, security scans and penetration tests;
- 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; and,

- 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 assessment shall be documented in a report that follows the NRC Template for the Risk Assessment Report. The report shall be delivered in draft form and then in final form after NRC comments are incorporated.

Any residual risk is tracked in the Plan of Action and Milestones (POA&M) Report. The POA&M Report documents the results of this process. POA&Ms 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 to remediate all high and moderate security findings, and track the remaining security findings using the system's POA&M Report.

Subtask 5: Systems Security Plan

The contractor shall perform this task as identified in the table found in section 3 "Scope of Work".

The SSP 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 SSP identifies the necessary security controls that are required, citing the security controls that are in place, those that are planned, those that are not 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 SSP shall be documented in a report that follows the NRC Template. The report shall be delivered in draft form and then in pre-system ST&E form after NRC comments are incorporated. The SSP shall be updated after completion of the ST&E test report to reflect validated in-place and planned controls.

Subtask 6: Preliminary Testing

The contractor shall perform a preliminary assessment of the system to ensure the system is compliant with federally mandated and NRC defined security requirements. The contractor shall identify any operational risks found that may affect the system's ability to perform its mission and protect its data (stored and transmitted). The contractor shall obtain from the system owner a list of deviations that have been approved by the Designated Approving Authorities (DAAs), so these risks can be factored in during testing. Accepted risks are still reported, evaluated, and documented.

This subtask includes the automated and manual testing of the different system platforms to ensure they have been configured, operated, and maintained correctly. Also, the contractor must ensure the entire system is tested including those components not identified in this SOW. This testing specifically excludes any Development/Test Environment.

The following is a list of some of the standards that must be checked:

- National Institute of Standards and Technology (NIST) Federal Information Processing (FIPS) 140-2. When checking NIST FIPS 140-2, the contractor must ensure that all cryptography used in the system has been validated, has a current FIPS 140-2 certificate, and the configuration of that cryptography complies with the security policy specified by the certificate for the cryptographic module.
- NIST 800-53 Rev 2 or later standard. The contractor must ensure the system complies with the technical, managerial, and procedural controls found in this standard.

- NRC Hardening Standards. The contractor must ensure the system meets all the NRC hardening standards. For a complete list of Hardening standards please see "<http://www.internal.nrc.gov/ois/it-security/guidance.html>".

The CSO has purchased a Center for Internet Security License for the NRC giving the organization the ability to access CIS Benchmarks; to distribute CIS Benchmark documents and tools; and to use CIS Benchmarks for commercial purposes.

Note: When a federally mandated configuration or NRC hardening standard have not been specified, the contractor will test that component using the vendor's suggested best security practices.

The contractor shall document the results and observations of this 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 the system owner to remediate all high/moderate security findings/risks and track those risks using a Plan of Action and Milestone (POA&M) Report.

The contractor shall be responsible for coordinating and executing all applicable site access and non-disclosure agreements and authority to scan forms with parties other than the Nuclear Regulatory Commission prior to commencement of the above mentioned activities, ensuring that project schedules are not impacted.

Subtask 7: ST&E Plan

The contractor shall perform this task as identified in the table found in section 3 "Scope of Work".

The ST&E plan exercises the system's 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 Guide for accessing the Security Controls in Federal Information Systems
- 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
- NRC System Security Test and Evaluation Plan Template

The ST&E plan provides detailed test procedures to ensure all federally mandated and NRC defined security requirements are fully tested. These procedures contain sufficient detail that a technically trained individual not familiar with the system can successfully follow the procedures.

The ST&E plan identifies all testing assumptions, constraints, and dependencies and includes a proposed schedule that identifies which personnel, hardware, software, and other requirements that must be met for each portion of the schedule to accomplish full system security testing of all system security functional and assurance requirements where the requirements are not stated as being fulfilled by another system. Also, the contractor shall ensure testing identifies any operational risks found that may affect the system's ability to perform its mission and protect its data (stored and transmitted). Additionally, the contractor must ensure the ST&E Plan includes the entire system.

The following test methods shall be used:

- **Analysis** - The "analysis" verification method shall be used to appraise a process, procedure, or document to ensure properly documented actions (e.g. risk assessments, audit logs, organization level policies, etc.) are in compliance with established requirements. An example of "analysis" as an evaluation technique would be to review documented physical security policies and procedures to ensure compliance with established requirements. This verification method is often called a documentation review.

- **Demonstration** - The contractor will observe random individuals to verify that activities on the system follow the documented procedure or process as the activity is performed. For example, observe visitors upon computer room entry in order to verify that all visitation procedures are followed.
- **Interview** - The contractor will interview personnel to verify the security policies and procedures are understood as implemented and prescribed by governing policies and regulations.
- **Inspection** - The contractor will ensure security controls have been properly implemented and maintained. For example, the contractor shall verify that the visitor's name, signature, organization, reason of visit, arrival and departure date, time, and the escort's name, initials, or signature are included on the log sheets.
- **Technical Test** - The Technical Test verification method shall be used to verify that each implemented control is functioning as intended. For example, the contractor will attempt to access the system by logging on to the system from an end user workstation (or other device) using an incorrect password to see if the system responds with an error message stating an incorrect password has been entered or denies access after exceeding the maximum threshold for logon attempts.

Testing requirements that are stated as being fulfilled by another system (provider) shall be accomplished by verifying that the provider system security plan in-place controls meet the requirement.

Subtask 8: System Testing

The contractor shall perform this task as identified in the table found in section 3 "Scope of Work".

The system shall be independently reviewed, verified, and validated using the system's security test plans and procedures to ensure the accuracy and adequacy of documented test procedures for all system security controls and security requirements and associated technical resolutions, risk mitigation, and implementations contained within various NRC security and systems development documentation or the Rational Suite Enterprise such that confirmation that the system and associated controls are operating as intended. Once testing has been completed, the ST&E Report, the Vulnerability Assessment Report, and the Corrective Action Plan shall be developed to document the results of the system's testing. Finally, the ST&E Plan is updated to reflect validated information.

Subtask 9: ATO Package

The contractor shall perform this task as identified in the table found in section 3 "Scope of Work".

The ATO package documents the results of the system certification and provides the authorizing official with the essential information needed to make a credible risk-based decision on whether to authorize operation of the information system.

The ATO Package contains the following deliverables plus a corresponding CD that contains all supporting documentation: Security Categorization Document, SRA, SSP, ST&E Plan, ST&E Report, Vulnerability Assessment Report, Corrective Action Plan, and an Approval to Operate Request Memo.

All documentation must be provided to the CSO in both hard copy and electronically in MS Word. The SSP must be current (within 2 months). The SRA, ST&E Plan, ST&E Report, and VAR must be current (within 2 months).

8.0 TRAVEL

The following travel is required to support this effort:

- IAS – travel is not required for this effort.

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.