

# ORDER FOR SUPPLIES OR SERVICES

PAGE 1 OF 8 PAGES


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

BPA NO. BASIC


1. DATE OF ORDER <b>MAY 19 2008</b>		2. CONTRACT NO. (If any) GS35F0229K		6. SHIP TO:	
3. ORDER NO. DR-33-06-317-T045		4. REQUISITION/REFERENCE NO. OIS-06-317 dtd: 4/23/2008		a. NAME OF CONSIGNEE U.S. Nuclear Regulatory Commission	
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				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.	
d. CITY ROCKVILLE	e. STATE MD	f. ZIP CODE 208506106		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 B&R:810-15-5D1-328 JC:J1100 BOC:252A APP:31X0200.810 FFS:10870663C OBLIGATE: \$225,000.00		10. REQUISITIONING OFFICE CIO 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 SMALLBUSINESS			
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>TASK ORDER 45 UNDER DELIVERY ORDER NO. DR-33-06-317 (CISSS): The contractor shall provide the U.S. Nuclear Regulatory Commission (NRC) with, "Annual Security Control Testing" in accordance with the following:</p> <ul style="list-style-type: none"> <li>- The attached Statement of Work (SOW)</li> <li>- The attached Schedule of Supplies or Services and Price/Cost</li> <li>- The terms and conditions of GSA Schedule No. GS35F0229K</li> <li>- The terms and conditions of NRC Delivery Order No. DR-33-06-317</li> </ul> <p>Reference: MAR Quotation (Ref# 2008-064/WA971), dtd: 5/15/08 DUNS: 062021639</p> <p>ACCEPTANCE:                        Signature Date                      Linda Klages, Vice President, Contracts                      Print Name/Title                 </p>					

SEE BILLING INSTRUCTIONS ON REVERSE	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						17(i). GRAND TOTAL \$249,958.14 (Ceiling)
	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				

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

TEMPLATE AMENDMENT  
FOR LOCAL DISTRIBUTION  
THIS EDITION NOT USABLE

SUNSI REVIEW COMPLETE

JUN 06 2008

OPTIONAL FORM NO. 346 (2/006)  
PRESCRIBED BY 41 CFR 101-11.6  
5010-108-01

**U.S. Nuclear Regulatory Commission**  
**Statement of Work for Task Order No. 45**  
**Under Delivery Order No. DR-33-06-317**  
**Annual Security Control Testing**

## **1.0 OBJECTIVE**

The objective of this task order is to obtain professional services to support the Nuclear Regulatory Commission (NRC) in its annual information systems security control testing consistent with National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 2, NIST SP 800-37, and the Office of Management and Budget (OMB) Federal Information Security Management Act (FISMA) guidance. Specifically, the contractor shall assist NRC in performing required annual security control testing for NRC systems.

## **2.0 BACKGROUND**

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

This activity will assist the NRC in ensuring adherence to federally mandated and NRC defined security requirements. Also, this activity will help the NRC to identify and understand the risks associated with operating these information systems.

For more information about annual control testing please see:

<http://csrc.nist.gov/publications/nistpubs/800-37/SP800-37-final.pdf> and  
<http://csrc.nist.gov/publications/drafts/800-53A/draft-SP800-53A-fpd-sz.pdf>

## **3.0 PERIOD OF PERFORMANCE**

The Annual Security Control Test Reports shall be coordinated with the system owners, accepted by CSO, and **completed by July 15, 2008**. The period of performance for this task order will be from date of award through January 27, 2009.

## **4.0 FUNDING**

- (a) The total estimated amount (ceiling) for the products/services ordered, delivered, and accepted under this task order is **\$249,958.14 (includes \$8,554.44 for NTE travel)**.
- (b) The amount presently obligated with respect to this task order is **\$225,000.00**. 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 above is done so at the Contractor's sole risk.

## **5.0 SCOPE OF WORK**

The Contractor shall provide all personnel, materials, hardware, software, labor, supplies, equipment, travel and other direct costs necessary to accomplish the performance of the activities described below to support the tasks specified in Statement of Work (SOW) Enclosure 6 of delivery Order DR-33-06-317 "Certification and Accreditation Process and Deliverables" for unclassified systems. If available, prior year self assessments and test results will be used as a reference, and tests performed under this task should leverage such previous work to the extent practicable.

### **Sponsor Office**

NRC Computer Security Office (CSO)

### **System Owner**

Multiple Offices in NRC (see Table 1 under Subtask 1 below).

### **System Description**

All operational NRC major applications, general support systems, and contractor facilities identified in the NRC FISMA Inventory which have not been reviewed as part of a formal Security Test and Evaluation since August 15, 2007. Those systems that are planned to be tested under other tasks orders prior to August 15, 2008 should not be proposed under this task. Refer to Subtask 1, Table 1 for list of systems to be tested.

### **Instructions for Deliverables**

Deliverables shall be consistent with period of performance in this statement of work and the detailed schedule required in Subtask 1. If for any reason a deliverable cannot be delivered within the specified time frame, the contractor shall notify the CSO (CSO project officer) in writing with cause and the proposed revised time frame. This notice shall include the impact on the overall project. The CSO 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 five (5) working 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 CSO. If revisions are required, the contractor has three (3) days to complete the revisions and submit the revised draft deliverable to the CSO. The three (3) day corrective action time will not include time in which the Contractor is waiting on the NRC for data necessary to perform the corrective action.

Once the deliverable is approved by CSO, the deliverable will become final. For each deliverable (draft or final), the contractor shall provide one (1) copy and one (1) electronic version of the deliverable to the CSO, 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, PowerPoint, or Excel (version 2003 or later version as approved by the CSO). Also, deliverables may be developed in PDF format. The templates used for each deliverable shall be developed by the contractor and approved by the CSO. Any changes to these templates must be approved by the CSO.

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 CSO.

### **Schedule**

The Contractor shall provide specific task deliverables consistent with the NRC-approved integrated project plan (Subtask 1). The period of performance is specified in Section 5.

## **6.0 SPECIFIC TASKS**

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

Develop and implement a project plan to ensure completion of the Annual Security Control Test Reports within the period of performance (identified in Section 5 below). The Contractor shall be required to develop and maintain an Integrated Security Activity Project Plan and perform Integrated Activity Scheduling for the program. These deliverables shall be developed at the individual system or site level (i.e., each system or site for which an Annual Security Control Test Report will be undertaken) and aggregate to the program level. The Microsoft Project Plan shall incorporate all tasks and projects such that the individual projects roll up into an Integrated Security project schedule encompassing all NRC security related activities, services, and deliverables. The Microsoft Project Plan shall identify resources for each activity and include the Work Breakdown Structure levels.

#### **The project plan will include:**

A Level 5 Work Breakdown Structure (WBS). The WBS shall include a definition of the work to be conducted decomposed into distinct discrete manageable tasks or groups of tasks (work packages) with decisive outputs and specific measurable entry and exit criteria. Each work package shall have a short duration, or can be divided into a series of milestones whose status can be objectively measured. Each work package shall be assigned a start and finish date, a budget value, and be integrated with higher-level schedules.

A schedule and budget for accomplishing the work identifying what resources are needed and how much effort will be required in what time frame to complete each of the tasks in the WBS. The Contractor shall allocate a portion of the budget for each work package that comprises the WBS, and ensure that the WBS adequately defines all work necessary to meet the requirements for the project.

An updated high-level summary report detailing the current expected start and completion dates for each system's testing and deliverables shall be made available to the CSO upon request.

The contractor shall keep CSO apprised of any actual or anticipated schedule delays or cost overruns.

## Subtask 2: System and Control Selection

Based upon the contractor's concurrent and prior work under other NRC task orders and in coordination with the CSO, the list of systems in Table 1 was developed per the criteria described in section 3.0 above (System Description). Any system with a "No" in the Tested column shall be tested as part of this task. The contractor shall use the Security Assessment Report template in Appendix I of NIST SP 800-53A (or other format suggested by the contractor and as approved by the CSO) as the basis for each system's Annual Security Control Test Report.

**Table 1**

Office	System	Type	Tested (* = testing underway or planned for FY08)	Notes
OIS	ADAMS	MA	Yes	ST&E Report dtd 11/16/07
OIS	DCS	GSS	Yes	ST&E Report dtd 9/26/07
<b>ASLBP</b>	<b>DDMS</b>	<b>MA</b>	<b>No</b>	<b>ST&amp;E Report dtd 8/10/07</b>
<b>OIS</b>	<b>Desktops</b>	<b>GSS</b>	<b>No</b>	
SECY	EHD	MA	Yes	ST&E Report dtd 10/05/07
				v2.4 Planned ST&E Report 8/19/08. (under another task order)
OIS	EIE	MA	Yes*	v3.5 No planned testing.
OIS	Email	GSS	Yes	ST&E Report dtd 12/1/07
NSIR	ERDS	MA	Yes	ST&E Report dtd 11/15/07
CFO	FEES	MA	Yes*	To be tested in FY08 (late summer, no set date thus far)
NMSS	GLTS	MA	Yes*	It will be tested in FY08 prior to 8/15/2008
<b>RES</b>	<b>HPCS</b>	<b>GSS</b>	<b>No</b>	
CFO	HRMS	MA	Yes*	Legacy - ST&E Report 5/29/08 (Schedule under revision, may shift to 5/16)
<b>OIS</b>	<b>IDSSD</b>	<b>GSS</b>	<b>No</b>	
<b>ADM</b>	<b>IPSS</b>	<b>MA</b>	<b>No</b>	
OIS	LAN/WAN	GSS	Yes	ST&E Report 9/13/07
<b>NMSS</b>	<b>LTS</b>	<b>MA</b>	<b>No</b>	
OIS	MPKI	GSS	Yes*	ST&E Report to be delivered 5/9/08
<b>OIS</b>	<b>Novell</b>	<b>GSS</b>	<b>No</b>	
OIS	NSICD	MA	Yes*	ST&E Report to be delivered 5/29/08

				ST&E Report dtd 11/06/07.
NSIR	OCIMS	MA	Yes	Updates to system require some retesting (next 60 days)
				On temporary hold. Schedule under revision. Baseline to HIGH, SSP not revised.
OIS	RAS	GSS	No	
NRR	RPS	MA	No	ST&E Report dtd 7/26/07
NSIR	SGI-LAN	GSS	No	ST&E Report sent final 5/29/07
OIS	TAC	GSS	No	
OIS	Telecom	GSS	No	
				Schedule under development, system C&A project not kicked off.
OIS	BASS	GSS	No	
OIS	Windows	GSS	No	
Other Gov Systems* and Contractor				
ADM	E-QIP*	MA	No	
ADM	FPDS-NG*	MA	No	
ASLBP	LSN	MA	Yes	ST&E Report dtd 8/17/07
CFO	FFS*	MA	No	
CFO	FPPS*	MA	No	
CFO	NIH*	GSS	No	
CFO	SPS*	MA	No	
NMSS	CNWRA	MA	Yes	ST&E Report dtd 1/15/08
OIS	L3-EER	GSS	No	
OIS	LMSSC	GSS	No	

*\* Other Gov Systems only require verification/evidence of testing by sponsoring agency*

The contractor shall develop selection criteria to determine which controls will be tested in accordance with NIST SP 800-53 (see control CA-7), NIST SP 800-37 and OMB FISMA guidance. 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 system POAM items. All other controls not tested under this task orders shall be planned to be tested at least once during the 3-year accreditation cycle. Upon selection criteria approval by the CSO, the contractor shall work with system owners and develop system specific plans for annual testing of controls (to include those tested under this task orders and those to be tested in subsequent years).

### Subtask 3: Control Testing and Reporting

Based upon the test plans developed in Subtask 2, the Contractor shall perform a comprehensive assessment of the selected management, operational, and technical security controls of the systems identified in subtask 2 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 each system consistent with NIST SP 800-53A. Prior to testing, the contractor shall hold a kickoff meeting with each system owner to review the scope of testing, controls selected, testing and documentation timeframes, required system owner support, and expected outcomes. Upon completion of testing the contractor shall develop Annual Security Control Test Report documentation for each system and incorporate any findings into each system's POAM.

Draft Annual Security Control Test Reports and the associated systems' POAM shall be submitted to the CSO for the purpose of coordination with the System owner. Upon System Owner review and comment, the contractor shall revise and update each Annual Security Control Test Report and POAM as appropriate and provide final versions to the CSO. A summary report shall be developed aggregating the findings across all systems. This summary Annual Security Control Test Report shall provide the CSO an overall view of the status of control implementation for all tested systems, as well as any observed vulnerability trends at an agency and system level with special attention to those deficiencies that would impact NRC FISMA compliance.

#### **Subtask 4: Test Result Upload**

Upon completion of Subtask 3, the contractor shall upload the test results and any resultant Plan of Action and Milestones (POAM) action items into the CSO control tracking tool.

### **7.0 TRAVEL**

Travel is required to the following locations:

U.S. NRC Region I  
475 Allendale Road  
King of Prussia, PA 19406-1415

U.S. NRC Region II  
Sam Nunn Atlanta Federal Center, 23 T85  
61 Forsyth Street, SW  
Atlanta, GA 30303-8931

U.S. NRC Region III  
2443 Warrenville Road  
Suite 210  
Lisle, Illinois 60532-4352

U.S. NRC Region IV  
Texas Health Resources Tower  
611 Ryan Plaza, Suite 400  
Arlington, TX 76011-4005

U.S. Nuclear Regulatory Commission  
Technical Training Center  
Osborne Office Center  
5746 Marlin Road, Suite 200  
Chattanooga, TN 37411-5677

Center for Nuclear Waste Regulatory Analyses (CNWRA)  
Southwest Research Institute  
6220 Culebra  
San Antonio, TX 78228-0510

One trip will be required to each location and shall be for 2 days and 1 night, for one security analyst. A not-to-exceed (NTE) line item of \$8,554.44 has been included for travel required for this effort. All travel will be reimbursed in accordance with DR-33-06-317, Section 4.3, Travel Requirements. All travel, other than local travel, requires the prior approval of the CSO.

## **8.0 MEETINGS**

The contractor's technical representative shall attend monthly status meetings at NRC Headquarters to discuss work being done under this task order.

## **9.0 LEVEL OF EFFORT**

The estimated level of effort for this task order is 2,118 staff hours.