

**ORDER FOR SUPPLIES OR SERVICES**

PAGE OF PAGES  
1 10

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

BPA NO. BASIC

1. DATE OF ORDER <b>SEP 16 2009</b>		2. CONTRACT NO. (If any)		6. SHIP TO:	
3. ORDER NO. DR-33-06-317-T074		4. REQUISITION/REFERENCE NO. 33-06-317T074 DTD 8/4/2009		d. 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 Debbs 11545 Rockville Pike Mail Stop: T-2-C-2	
7. TO:		c. CITY Washington		d. STATE DC	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 SUITE 204				<input type="checkbox"/> a. PURCHASE <input checked="" type="checkbox"/> b. DELIVERY 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		
9. ACCOUNTING AND APPROPRIATION DATA ACCOUNTING AND APPROPRIATION DATA ON CONTINUATION SHEET 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"/> 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)	
a. INSPECTION Rockville, MD		b. ACCEPTANCE Rockville, MD		16. DISCOUNT TERMS	

17. SCHEDULE (See reverse for Rejections) See CONTINUATION Page

ITEM NO. (a)	SUPPLIES OR SERVICES (b)	QUANTITY ORDERED (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)	QUANTITY ACCEPTED (g)
	TASK ORDER 74 UNDER NRC ORDER DR-33-06-317 (CISSS): The contractor shall provide the U.S. Nuclear Regulatory Commission (NRC) with, "Computer Security Office (CSO) Information Security Program (ISP) Support & Incident Response" services in accordance with the following:  -The attached Statement of Work (SOW) -The attached Schedule of Supplies and/or Services and Price -The terms and conditions of GSA Schedule GS-35F-0229K -The terms and conditions of NRC Order No. DR-33-06-317 Reference: MAR Quotation (Ref #2009-116/WA1530), dtd 9/9/09  ACCEPTED:  Signature Linda Klages, VP, Contracts Print/Name and Title Date: 09/16/2009					

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

AUTHORIZED FOR LOCAL REPRODUCTION  
PREVIOUS EDITION NOT USABLE

OPTIONAL FORM 347 (REV. 4/2008)  
PRESCRIBED BY GSA/FAR 48 CFR 63.213(f)

TEMPLATE - ADM001

SUNSI REVIEW COMPLETE

SEP 22 2009

ADM002

**ORDER FOR SUPPLIES OR SERVICES  
SCHEDULE - CONTINUATION**

PAGE NO.  
2

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

DATE OF ORDER

CONTRACT NO.

ORDER NO.

DR-33-06-317-T074

ITEM NO. (A)	SUPPLIES OR SERVICES (B)	QUANTITY ORDERED (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)	QUANTITY ACCEPTED (G)
	ACCOUNTING AND APPROPRIATION DATA:  97S-15-5D1-328 N7343 252A 31X0200 FFS# CS009334 OBLIGATE: \$105,397  97S-15-5D1-328 N7343 252A 31X0200 FFS# CS009342 OBLIGATE: \$125,1000  925-15-171-107 Q4171 252A 31X0200 FFS# 09631700171_0804a OBGLIATE: \$150,000					

TOTAL CARRIED FORWARD TO 1ST PAGE (ITEM 17(H))

**DELIVERY ORDER DR-33-06-317**

**TASK ORDER (74)**

**Computer Security Office (CSO)**

**Information Security Program (ISP) Support and Incident Response**

**1.0 OBJECTIVE**

The Contractor shall support the Nuclear Regulatory Commission (NRC) in its efforts to develop and implement the organization's Information Security Program.

**2.0 SCOPE OF WORK**

The Contractor must ensure NRC's Information Security Program meets federally mandated and NRC defined security requirements. The Contractor shall provide the following services to the CSO:

- Provide Integrated Project Planning and Activity Scheduling
- Assist in Establishing and Maintaining a Continuous Monitoring Program
- Assist in Establishing and Maintaining a Compliant Incident Response Program
- Provide Communications Support
- Provide Security Engineering Support
- Information Security Program Support

The Contractor shall provide the necessary security support staff to meet the requirements specified in this Statement of Work (SOW).

**3.0 PERIOD OF PERFORMANCE**

This task order will have a period of performance of one year with one (1) one-year option.

Period	From	To	Condition
Base Year	Sept 18, 2009	Sept 17, 2010	None
Option Year 1	Sept 18, 2010	Sept 17, 2011	Only Applicable if Option Year of Base Contract is Exercised

**4.0 FUNDING**

- (a) The total estimated amount (ceiling) for the products/services ordered, delivered, and accepted under this task order is **\$708,948.00** (includes **\$10,000** for NTE travel).
- (b) The amount presently obligated with respect to this task order is **\$380,397.00**. 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.

## 5.0 TASKS

The Contractor shall support the organization according to the schedule of supplies, services, and prices found in the Consolidated Information Security Support Services (CISSS) contract terms Enclosure 6 Section B.

**Note: At no time is the Contractor allowed to configure an NRC operational system.**

### **Subtask 1: Provide Integrated Project Planning and Activity Scheduling**

The project plan shall include an integrated Level 5 Work Breakdown Structure (WBS) across all task orders that have been defined under the contract. 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 be assigned a start and finish date, a budget value, and is integrated with the project plans from other task orders.

Also, the project plan shall provide resource utilization information that identifies the budget to accomplish the work, the resources needed to complete the work, and the effort required in the specified time frame for the completion of 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.

Microsoft Project Plan that incorporates 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.

### **Subtask 2: Assist in Establishing and Maintaining a Continuous Monitoring Program**

The Contractor shall assist the NRC in establishing and maintaining a continuous monitoring program that addresses federally mandated and NRC defined security requirements. The Contractor shall assist the NRC in reporting the status of the continuous monitoring program to the Office of the Inspector General (OIG) and other government agencies. At a minimum, the NRC continuous monitoring program must address the following elements:

- Plan of Action and Milestone (POA&M) Resolution and Reporting (Quarterly)
- Contingency Planning (Annually)
- Updating Security Documentation (Annually)
- Controls Testing (Annually)
- System Scanning (Quarterly)

At least annually, the Contractor shall review NRC's continuous monitoring program to ensure the program continues to address requirements.

**Subtask 3: Assist in Establishing and Maintaining a Compliant Incident Response Program**

The Contractor shall assist the NRC in developing, establishing, and maintaining an agency wide Incident Response Program that addresses federally mandated and NRC defined security requirements (found in Management Directives and policy).

At a minimum the Incident Response Program shall satisfy the following controls:

- **IR-1 INCIDENT RESPONSE POLICY AND PROCEDURES** - The organization develops, disseminates, and reviews/updates a formal, documented incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and formal, documented procedures to facilitate the implementation of the incident response policy and associated incident response controls.
- **IR-2 INCIDENT RESPONSE TRAINING** - The organization trains personnel in their incident response roles and responsibilities with respect to the information system; and provides refresher training annually. Also, the organization incorporates simulated events into incident response training to facilitate effective response by personnel in crisis situations. Also, the organization employs automated mechanisms to provide a more thorough and realistic training environment.
- **IR-3 INCIDENT RESPONSE TESTING AND EXERCISES** - The organization tests and/or exercises the incident response capability for the information system annually using organization-defined tests and/or exercises to determine the incident response effectiveness and documents the results. Also, the organization employs automated mechanisms to more thoroughly and effectively test/exercise the incident response capability.
- **IR-4 INCIDENT HANDLING** - The organization implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery; coordinates incident handling activities with contingency planning activities; and incorporates lessons learned from ongoing incident handling activities into incident response procedures and implements the procedures accordingly. Also, the organization employs automated mechanisms to support the incident handling process. Also, the organization includes dynamic reconfiguration of an information system as part of the incident response capability. Also, the organization identifies classes of incidents (e.g., targeted malicious attacks, untargeted malicious attacks, malfunctions due to design or implementation errors and omissions) and defines appropriate actions to take in response to ensure continuation of mission/business operations. Also, the organization correlates incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response. Also, the organization implements a configurable capability to automatically disable an information system if a set organization defined security violations are detected.
- **IR-5 INCIDENT MONITORING** - The organization tracks and documents information system security incidents. Also, the organization employs automated mechanisms to assist in the tracking of security incidents and in the collection and analysis of incident information.
- **IR-6 INCIDENT REPORTING** - The organization requires personnel to report suspected security incidents to the organizational incident response capability and must report security incidents to designated authorities. Also, the organization employs automated mechanisms to assist in the reporting of security incidents. Also, the organization reports information system weaknesses, deficiencies, and/or vulnerabilities associated with reported security incidents to appropriate organizational officials.
- **IR-7 INCIDENT RESPONSE ASSISTANCE** - The organization provides an incident response support resource that offers advice and assistance to users of NRC information systems for the handling and reporting of security incidents. Also, the organization employs automated mechanisms to increase the availability of incident response-related information and support. Also, the organization establishes a

direct, cooperative relationship between its incident response capability and external providers of information systems protection capability and identifies organizational incident response team members to the external providers.

- **IR-8 INCIDENT RESPONSE PLAN** - The organization develops an incident response plan that provides the organization with a roadmap for implementing its incident response capability; describes the structure of the incident response capability; provides a high-level approach for how the incident response capability fits into the overall organization; meets the unique requirements of the organization, which relate to mission, size, structure, and functions; defines reportable incidents; provides metrics for measuring the incident response capability within the organization; defines the resources and management support needed to effectively maintain and mature an incident response capability; and is reviewed and approved by designated officials within the organization. The organization distributes copies of the incident response plan to specified personnel. The organization reviews the incident response plan annually. The organization revises the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing. The organization communicates any changes to the incident response plan to specified personnel.

#### **Subtask 4: Provide Communications Support**

The Contractor shall support CSO's efforts to communicate NRC policy, standards, procedures, guidance, and security related requirements to management and the NRC user community. The contractor will develop presentations, demonstrations, and briefings to support this effort. The contractor may be called upon to provide technical support and expertise during these activities.

#### **Subtask 5: Information Security Program Support**

The Contractor shall support the CSO in the development, implementation, and continuous improvement of the agency's Information Security Program and work with the CSO to address risks/deficiencies in the program in a timely and effective manner. An Information Security Program includes the following: security policies, incident handling, capital planning, information system development life cycle, certification and accreditation, continuous monitoring, contingency planning, system inventory, and maintenance of a security documentation repository.

The following identifies the support the contractor will provide under this subtask:

- The Contractor shall support NRC's efforts to certify and accredit its information systems.
- The Contractor shall support NRC's efforts to establish a contingency planning process that addresses the needs of the agency.
- The Contractor shall support NRC staff in the development and documentation of security controls and security requirements and associated technical resolutions, risk mitigation, and implementations.
- The Contractor shall support NRC's efforts to review, verify, and validate security controls & requirements and associated technical resolutions, risk mitigation, and implementations contained within various NRC information system both in production and under development.
- The Contractor shall support the functional alignment of common security control sets and standard operating procedures consistent with FISMA and NIST SP 800-53 that integrates with the NRC's Project Management Methodology.
- The Contractor shall support the NRC in developing a security line of business program and supporting the agency in assessing, documenting, and implementing common security solutions.
- The Contractor shall assist the NRC in meeting its FISMA reporting requirements.

**DR-33-06-317-T074**

- The Contractor shall assist the NRC in responding to Data Calls by the Office of Inspector General (OIG) and other government agencies.
- The Contractor shall provide support services to develop, implement, and load automated tools that support NRC's Information Security Program. This includes support for Capital Planning and Investment Control (CPIC), assisting with tool selection, Certifying and Accrediting tools, and entering security information into the tools for reporting and trend analysis.

**Subtask 6: Provide Security Engineering Support**

The Contractor shall provide Security Engineering support to verify and validate that proposed 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.

**6.0 TRAVEL**

Travel may be required for this effort and should not exceed \$10K per year.

**7.0 MEETINGS**

As needed, the Contractor's Project Manager and technical lead shall attend status meetings at NRC Headquarters to discuss issues and work being performed under this task order.

**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.

**DELIVERY ORDER: DR-33-06-317  
TASK ORDER: DR-33-06-317-T074  
SCHEDULE OF PRICE AND/OR COST**

BASE YEAR TOTAL \$ 708,948.00  
 OPTION YEAR TOTAL \$ 735,408.32  
**GRAND TOTAL \$ 1,444,356.32**

**Base Year - Option Year 3 Rates**

Task Order Mapping	Schedule B Item Number	SOW/REF	DELIVERABLE TITLE AND REQUIRED LABOR CATEGORIES FOR COMPLETION OF 1 DELIVERABLE FOR 1 SYSTEM	DISCOUNTED GSA LABOR RATE	HOURS FOR MAJOR SYSTEM	TOTAL AMOUNT FOR MAJOR SYSTEM	TO For reasons provided in Task Order Response	
							Hours	Dollars
2	3	8.0	<b>CONTROLS AND REQUIREMENTS (ANNUAL)</b>					
			Project Manager	\$				
			QA Manager	\$				
			Security Specialist IV	\$				
			Security Specialist II	\$				
			Technical Expert II	\$				
			Technical Expert I	\$				
			Technical Writer II	\$				
			Technical Writer I	\$				
			<b>TOTALS FOR CONTROLS AND REQUIREMENTS (ANNUAL)</b>					<b>139,238.61</b>
3	3	8.0	<b>CONTROLS AND REQUIREMENTS (ANNUAL)</b>					
			Project Manager	\$				
			QA Manager	\$				
			Security Specialist IV	\$				
			Security Specialist II	\$				
			Technical Expert II	\$				
			Technical Expert I	\$				
			Technical Writer II	\$				
			Technical Writer I	\$				
			<b>TOTALS FOR CONTROLS AND REQUIREMENTS (ANNUAL)</b>					<b>141,993.57</b>
4	16	End 6	<b>SECURITY COMMUNICATIONS SUPPORT (ANNUAL)</b>					
			Project Manager	\$				
			QA Manager	\$				
			Security Specialist IV	\$				
			Technical Expert II	\$				
			Technical Expert I	\$				
			Technical Writer II	\$				
			Technical Writer I	\$				
			<b>TOTALS FOR SECURITY COMMUNICATIONS SUPPORT (ANNUAL)</b>					<b>139,238.61</b>
5	7	8.0	<b>SECURITY CONTROL MAINTENANCE (ANNUAL)</b>					
			Project Manager	\$				
			QA Manager	\$				
			Security Specialist IV	\$				
			Technical Expert II	\$				
			Technical Expert I	\$				
			Technical Writer II	\$				
			Technical Writer I	\$				
			<b>TOTALS FOR SECURITY CONTROL MAINTENANCE (ANNUAL)</b>					<b>139,238.61</b>

6	8	8.0	SECURITY ENGINEERING (ANNUAL)					
			Project Manager	\$				
			QA Manager	\$				
			Security Specialist IV	\$				
			Senior INFOSEC Engineer	\$				
			Technical Expert II	\$				
			Subject Matter Expert III	\$				
			Technical Writer II	\$				
			Technical Writer I	\$				
			TOTALS FOR SECURITY ENGINEERING (ANNUAL)					\$ 139,238.81

BASE YEAR LABOR TOTAL \$ 698,948.00  
 BASE YEAR TRAVEL \$ 10,000.00  
 BASE YEAR GRAND TOTAL \$ 708,948.00

Option Year - Option Year 4 Rates

SOW REF	DELIVERABLE TITLE AND REQUIRED LABOR CATEGORIES FOR COMPLETION OF 1 DELIVERABLE FOR 1 SYSTEM	DISCOUNTED GSA LABOR RATE	HOURS FOR MAJOR SYSTEM	TOTAL AMOUNT FOR MAJOR SYSTEM	TO	
					For reasons provided in Task Order Response	
					Hours	Dollars
2	3	8.0	CONTROLS AND REQUIREMENTS (ANNUAL)			
			Project Manager	\$		
			QA Manager	\$		
			Security Specialist IV	\$		
			Security Specialist II	\$		
			Technical Expert II	\$		
			Technical Expert I	\$		
			TOTALS FOR CONTROLS AND REQUIREMENTS (ANNUAL)			\$ 145,081.66
3	3	8.0	CONTROLS AND REQUIREMENTS (ANNUAL)			
			Project Manager	\$		
			QA Manager	\$		
			Security Specialist IV	\$		
			Security Specialist II	\$		
			Technical Expert II	\$		
			Technical Expert I	\$		
			TOTALS FOR CONTROLS AND REQUIREMENTS (ANNUAL)		49,009.37	\$ 145,081.66
4	16	End 6	SECURITY COMMUNICATIONS SUPPORT (ANNUAL)			
			Project Manager	\$		
			QA Manager	\$		
			Security Specialist IV	\$		
			Technical Expert II	\$		
			Technical Expert I	\$		
			Technical Writer II	\$		
			TOTALS FOR SECURITY COMMUNICATIONS SUPPORT (ANNUAL)			\$ 145,081.66

5

7

8.0 SECURITY CONTROL MAINTENANCE (ANNUAL)	
Project Manager	\$
QA Manager	\$
Security Specialist IV	\$
Technical Expert II	\$
Technical Expert I	\$
<b>TOTALS FOR SECURITY CONTROL MAINTENANCE (ANNUAL)</b>	
	\$ 145,081.66

6

8

8.0 SECURITY ENGINEERING (ANNUAL)	
Project Manager	\$
QA Manager	\$
Security Specialist IV	\$
Senior INFOSEC Engineer	\$
Technical Expert II	\$
Subject Matter Expert III	\$
Technical Writer II	\$
<b>TOTALS FOR SECURITY ENGINEERING (ANNUAL)</b>	
	\$ 145,081.66

OPTION YEAR LABOR TOTAL \$ 725,408.32  
 OPTION YEAR TRAVEL \$ 10,000.00  
 OPTION YEAR GRAND TOTAL \$ 735,408.32