

**ORDER FOR SUPPLIES OR SERVICES**

PAGE OF PAGES

1 12

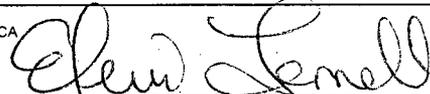
IMPORTANT: Mark all packages and papers with contract and/or order numbers.

BPA NO. BASIC

1. DATE OF ORDER <b>SEP 19 2008</b>		2. CONTRACT NO. (if any) GS35F0229K		6. SHIP TO:		
3. ORDER NO. DR-33-06-317-T052		MODIFICATION NO.		a. NAME OF CONSIGNEE U.S. Nuclear Regulatory Commission		
4. REQUISITION/REFERENCE NO. 33-06-317 T052		FFS #RQCS008303		b. STREET ADDRESS Attn: Bill Dabbs 11545 Rockville Pike Mail Stop: T2-C2		
5. ISSUING OFFICE (Address correspondence to) U.S. Nuclear Regulatory Commission Div. of Contracts Attn: Michele Sharpe Mail Stop: TWB-01-B10M Washington, DC 20555				c. CITY Washington		e. ZIP CODE 20555
7. TO:				d. STATE DC		
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 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.		<input checked="" type="checkbox"/> b. DELIVERY Except for billing instructions on the reverse, this delivery order is subject to instructions contained on this side only of this form and is issued subject to the terms and conditions of the above-numbered contract.
d. CITY ROCKVILLE		e. STATE MD	f. ZIP CODE 208506106		10. REQUISITIONING OFFICE CIO OIS/CSO	
9. ACCOUNTING AND APPROPRIATION DATA B&R: 87S-15-5D1-328 JC: N7343 BOC: 252A APPN NO.: 31X0200.87S OBLIGATE: \$604,428.68 DUNS# 062021639				\$604,428.68		
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"/> d. WOMEN-OWNED	<input type="checkbox"/> e. HUBZone	<input type="checkbox"/> f. EMERGING SMALL BUSINESS	<input type="checkbox"/> g. SERVICE-DISABLED VETERAN-OWNED
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		9/17/08-9/16/09		NET 30	
17. SCHEDULE (See reverse for Rejections)						

ITEM NO. (a)	SUPPLIES OR SERVICES (b)	QUANTITY ORDERED (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)	QUANTITY ACCEPTED (g)
	TASK ORDER 52 UNDER NRC ORDER DR-33-06-317 (CISSS): The Contractor shall provide the U.S. Nuclear Regulatory Commission with, "Enterprise Risk Assessment and Penetration Test" services in accordance with the following:  - The attached Statement of Work - The attached Schedule of Supplies or Services and Prices - The terms and conditions of GSA Schedule GS-35F-0229K - The terms and conditions of NRC Order DR-33-06-317  Reference MAR Quotation (Ref# 2008-101/WA971), dated 9/5/2008, entitled Task Order 052  ACCEPTANCE:  Signature _____ Date <u>9/25/2008</u>  Linda Klages/VP, Contracts Print Name/Title MAR, Incorporated					

SEE BILLING INSTRUCTIONS ON REVERSE	18. SHIPPING POINT		19. GROSS SHIPPING WEIGHT		20. INVOICE NO.		\$604,428.68 (OBLIGATED)	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				\$604,428.68 (CEILING)	17(i). GRAND TOTAL
	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	
--	--	---	--



DELIVERY ORDER NO. DR-33-06-317

TASK ORDER NO. DR-33-06-317-T052

ENTERPRISE RISK ASSESSMENT AND PENETRATION TEST

---

## 1.0 OBJECTIVE

Risk, as analyzed with a security perspective, has become a source of information that influences enterprise management strategy, which has a material impact, if not properly managed on all agency mission and program areas. The Enterprise Risk Assessment and Penetration Testing Task Order will serve as an independent assessment of the security posture of the Nuclear Regulatory Commission (NRC) to provide the Chief Security Office with an objective assessment so that proper resources can be applied and prioritized to correct system and infrastructure weaknesses and deficiencies.

The Enterprise Risk Assessment will have a demonstrative and positive impact on the effectiveness of NRC programs. The recently established Computer Security Office (CSO) has been tasked with defining and implementing a risk management approach focused on security to evaluate risks inherent within the agency's key operational elements that drive its mission. The Contractor shall develop a repeatable risk assessment penetration testing process and provide the Government with a plan that meets or exceeds the security testing standards identified in the National Institute of Technology Special Publication 800-42, Guideline on Network Security Testing and the Open Source Security Testing Methodology Manual (OSSTMM) referred to by the NIST in SP 800-42 to ensure that at a minimum, the test incorporates an assessment of the NRC information and data controls, personnel security awareness levels, fraud and social engineering control levels, computer and telecommunications networks, wireless devices, mobile devices, physical security access controls, security processes, and physical building controls, which if not present or acting as an effective deterrent could subject the Agency to the risk of information system compromise or embarrassment. This process begins with a common understanding of the rationale behind the initiative, objectives, and plans that define the necessary assessment and testing detail down to the individual input level, and with test expectations and test deliverables that are acceptable to the Chief Security Office.

The Contractor shall perform an internal and external penetration test on the NRC. The systems targeted for testing, the type of tests that are to be used, and the equipment/tools utilized during the test must be approved by the NRC.

## 2.0 Background

### Enterprise Risk Assessment

Within the 2007 "Inspector General's Assessment of the Most Serious Management and Performance Challenges Facing the NRC", item number five in the IG Assessment was characterized as "Implementing Information Technology". A more specific summary directs the aim towards the "upgrade and modernization of the NRC's Information Technology (IT) capabilities both for employees and for public access to the regulatory process." Recognizing the need to modernize, the NRC established goals to improve the "productivity, efficiency, and effectiveness of agency programs and operations, and enhance the use of information for all users inside and outside the agency."

This challenge presents opportunities beyond the acknowledged goals and drivers that have been identified as part of the upcoming growth and general modernization period. The broad, agency-wide impact of these goals requires efficient and effective executive management strategy and decisions. The scope serves as an example of an enterprise project area that would benefit from a NRC Enterprise Risk Assessment.

The following outputs will be generated during the Enterprise Risk Assessment

- Agency Mission Assessment.
- Evaluation Criteria.
- Breakdown of Security Functions and Touch Points.
- Gap Analysis.
- Enterprise Risk Assessment Report.
- Enterprise Risk Assessment Process.

Output from a NRC Enterprise Risk Assessment Process will feed directly into planning and continuous monitoring activities as the agency creates a chartable course using executive management directives to improve alignment and coordination. A consensus understanding of priorities will be established to provide a unified picture of risk, the corresponding boundaries and expectations of acceptance, and a continuum of actions to improve the organization's ability to meet its mission objectives and manage risks effectively.

### **Penetration Testing**

The Contractor will deliver a consolidated Penetration Test Report specifying the vulnerabilities and deficiencies found during the system wide penetration test. The NRC will select the systems and types of tests that are to be run. The penetration test will be broken into three phases:

- External – During this phase, the Contractor will test the NRC's ability to resist, detect, and respond to external threats.
- Internal – During this phase, the Contractor will evaluate the deficiencies and risks found in NRC's infrastructure.
- Social Engineering – During this phase, the Contractor will evaluate the NRC's susceptibility to a social engineering attack.

### **Presentation**

The Contractor will develop a presentation for management that summarizes the findings from the Enterprise Risk Assessment and the agency wide Penetration Test. This presentation will identify the path forward.

## **3.0 Scope of Work**

The Enterprise Risk Assessment and the Penetration Test will form the basis for a NRC Continuous Risk Management Program. The project is bound by an expectation that the results will provide a majority of the input necessary to construct pertinent follow-up actions and seed the overarching NRC Continuous Risk Management Program strategy.

The Contractor shall provide the necessary security support staff to address the tasks outlined in this task order based on ENCLOSURE 6 of Delivery Order DR-33-06-317 "CERTIFICATION AND ACCREDITATION PROCESS AND DELIVERABLES" for unclassified systems

### **3.1 Enterprise Risk Assessment**

The Contractor will perform an Enterprise Risk Assessment that addresses Recommendation 6 "Perform risk management at an enterprise level and outside of C&A" found in the Software Engineering Institute's (SEI) Report on the organization Information System Security (ISS) Program.

The Contractor must develop a method or process the NRC can use to obtain an enterprise risk management view of information management and security. This should be considered a multi-year objective, where the

input and output requirements of risk management at the NRC are enumerated, analyzed for gaps, and then tied to programs for improvement and implementation. The process of certification and accreditation provides system-specific risks that can and should be translated into mission and business risk, but at present do not. More important, the current collection of federal guidance does not provide a clear way to manage risks across systems, nor is there a method specified to allow organizations to "manage to impact" based on the severity of potential harm.

An enterprise-focused process of "planning-doing-checking-acting" would serve the NRC well. The creation of this process should not be designed without the input of all stakeholders charged and responsible for protecting mission critical information.

The following subtasks will be utilized during the Enterprise Risk Assessment.

### **3.1.1 Agency Mission Statement**

The Agency Mission Statement is the initial task the Contractor must perform so the NRC's mission and its objectives are completely understood. These objectives may be strategic, operational, or pertain to reporting or compliance. The Agency Mission Statement will be developed by interviewing appropriate senior executives and reviewing existing relevant documentation with the objective of identifying the following:

- Agency mission and program support planning details.
- Key stakeholders, internal and external customers of NRC.
- Critical services that support missions, stakeholders and customers as well as the systems and processes that support these services.
- An examination of how the critical services intersect and impact NRC business.
- Drivers, parameters and objectives associated with the Agency mission and program support areas.

The knowledge assembled from this effort will provide a complete picture of how NRC does business; the stakeholders, the critical support services and what factors affect the outcomes. The output will;

- Provide an immediate measure of prioritization.
- Guide deeper inspection of the security functions or service touch points of related assets, systems, and physical elements as well as processes and communication workflow to uncover vulnerabilities and associated risks.
- Broadly influence future risk assessment evaluations as well as NRC business decisions.

### **3.1.2 Evaluation Criteria**

The Contractor will develop baseline evaluation criteria for identifying potential security related events from in-place assets, systems, services, processes, and people that can positively or negatively impact achievement of NRC's corporate mission/ program objectives.

The Evaluation Criteria will provide the Contractor with meaningful measures to conduct a risk assessment breakdown of security functions or service touch points within business support services and document vital gaps that present a clear picture of enterprise risk and associated impact.

### **3.1.3 Breakdown of Security Functions & Touch Points**

Using the Agency Mission Statement to categorize and prioritize mission area support services, the Contractor will meet with program managers and key operational staff. Information collected during this effort will identify and categorize specific program risks emanating from product, process, management, resources, and other constraints. Additionally, centralized security service organizations will be assessed as standalone business

units as well as their cross-connected service lines. The type of input from these interviews that would play a part in this analysis could, as an example, include:

- Additional detail related to various business support services that did not surface in the interviews during the mission assessment.
- Workflow diagrams.
- An architectural perspective of systems, processes and the budgets that impact them.
- Past issues and corrective actions taken.
- Current issues and concerns.
- Additional organizational structure, roles and responsibilities, previously identified and agreed upon operational limitations, known gaps and other relevant metrics or measures.
- Impact of policy, reporting and compliance responsibilities.

At this stage of the Enterprise Risk Assessment, the gaps will start to come into focus. Evaluation criteria used in the assessment that reveals an attribute, disruption, misalignment, compliance failure or other type of problem with direct security functions or service touch points within business support service areas will raise a red flag that will provide input into the subsequent gap analysis step.

### **3.1.4 Gap Analysis**

The Contractor will perform a Gap Analysis to visualize an agency-wide, security focused, status baseline. A gap analysis provides the setting through which all vulnerabilities, risks, mitigations and outcomes are viewed and utilized for management decisions. The output from the gap analysis will drive executive decisions on investments, consolidation, auditing, monitoring, and other actions that reduce the risks to the agency's mission and program objectives.

At a minimum the gap analysis will;

- Identify vulnerabilities stemming from apparent misalignment, compliance issues, workflow, communication, security and others.
- Present the threat to the high priority mission support services as a result of the vulnerabilities. It is here that productivity, corporate investments, workforce alignment, and system/process issues associated with security functions and service touch points will be correlated with relative weights to the potential for disrupting the mission.
- Report on the conditions, events and roadblocks; procedural, communications, organizational, systems, workflow, that create the gap between current state and successful outcomes
- Forecast the areas of greatest need and as well as the related details that define criteria to assess how acceptable the associated investment and risks are

The Gap Analysis may provide answers to sample questions, such as;

- Are the gaps rooted in issues with communication and clarity of NRC objectives?
- Is a specific organizational area misaligned with NRC objectives from a management, resource, strategy, and data integrity or implementation perspective?

### **3.1.5 Enterprise Risk Assessment Report**

The Contractor will develop an Enterprise Risk Assessment Report that contains a unified picture of security focused risks associated with NRC assets, systems, and physical components that have security considerations as well as inter and intra-agency processes, communications, and service touch points that

come into contact with the NRC. The report can be used to guide decision making, outline effective collaboration, and build efficient plans towards effective achievement of NRC mission objectives.

Using the gap analysis output to select a NRC mission area in need of risk management mitigation, planning, monitoring and implementation, the Contractor will perform a business impact study against that mission area. Independent, technically sound evaluations of options presented for risk responses are vital to immediate success as well as appropriate future modeling and planning for other effected business areas. The Contractor shall develop a set of actions to align risks with mission, resources, and risk tolerance. The Contractor will further analyze processes and actions developed towards mitigating risks and work with the impacted functional area to implement actions and develop a plan to monitor, evaluate, and re-assess the implementation and effectiveness of response actions, which appropriately and proactively respond to these risks.

### 3.1.6 Enterprise Risk Assessment Process

The Enterprise Risk Management Process developed and documented by the Contractor will allow the NRC to monitor potential negative events to its assets, with the aim of ensuring the achievement of the agency's corporate mission and its program objectives.

The Enterprise Risk Assessment will be used to:

- Document the agency's risk appetite, identifying criteria for the agency's risk tolerance.
- Develop "as-is" and "to-be" state documents for enterprise risk management with design plans to close the gaps.
- Analyze enterprise impact criteria.
- Make informed business decisions.
- Monitor for opportunities to improve the process.

### 3.2 Penetration Testing

The Contractor shall conduct external penetration tests, internal penetration tests, and social engineering tests against the NRC infrastructure and its user community. The Contractor shall use a variety of testing tools, manual and automatic, including proprietary and modified open source, to attempt to penetrate NRC systems. In order to conduct this testing, the Contractor shall procure, lease, or borrow the commercially available tools needed to complete the testing. A designated government official must be present during all active penetration testing activities.

The following steps will be followed:

- **Phase 1: Information Gathering Tools** – The contractor shall develop a Tools Report that identifies the automated tools that are going to be used for information gathering. The tools report must be approved by the NRC before the Contractor can move on to the next phase.
- **Phase 2: Information Gathering** – The contractor shall gather information and perform an analysis identifying the touch points that need to be tested (for example: Routers, Firewalls, Gateways, Remote Access Services, Web Applications, Adherence to policies & standards, etc.).
- **Phase 3: Testing Tools** – The contractor shall develop a Tools Report that identifies the automated tools that are going to be used for testing. The tools report must be approved by the NRC before the Contractor can move on to the next phase.

The contractor shall update all devices that are going to be used during the tests with the latest patches, security updates, device drivers, and plug-ins. The devices used during the tests will be wiped once the tests have been completed.

- **Phase 4: Test Plan** - The contractor shall develop a detailed Test Plan that describes the external penetration testing, internal penetration testing, and social engineering attacks that are going to be performed against the NRC. The Test Plan must be approved by the NRC before any testing can be initiated. The Test Plan will answer the following questions:
  - Who will be performing the test?
  - What tools are going to be used?
  - What tests are going to be run against the NRC's automated information systems and user community?
  - When are the tests going to be run (date and time)?
  - Where will the tests be conducted from?
  - How are NRC automated information systems and users going to be affected?
  - How is contractor going to identify the risk?
- **Phase 5: Testing** - The contractor will perform external penetration testing, internal penetration testing, and social engineering attacks against the NRC under observation by a designated government official. All raw scans, observations, and testing results will be captured and documented in the corrective action report.
- **Phase 6: Corrective Action Report** – The Corrective Action Report shall contain but will not be limited to the following:
  - Summarize how the tests were performed and how risk was evaluated.
  - Identify the type of test that was run (external penetration test, internal penetration test, and social engineering attack).
  - Specify the hosts/users that were tested and the information systems/organizations they belonged to
  - Describe the vulnerabilities and deficiencies that were discovered during testing.
  - Identify the risks associated with these vulnerabilities and deficiencies. Risks will be organized with the most significant risk listed first.
  - Provide recommendations on how to mitigate these risks. A recommendation will be provided for every risk.
- **Phase 7: Cleanup** – The contractor shall wipe all devices used during testing and certify in writing that the task was completed. All contractors associated with this task order will sign non-disclosure agreements and not publish, discuss or otherwise communicate the test findings to individuals outside the NRC without rewritten authorization by the Government.

The Contractor will not conduct any testing without written the approval from the NRC and without being under a designated government official's observation.

**3.3 Presentation**

The Contractor will develop a presentation designed for department heads and other senior executives that summarizes the findings of the Enterprise Risk Assessment and Agency Wide Penetration Test with the goal of identifying the current risks to NRC information systems and their information. Also, the presentation will help department heads and other senior executives have a better understanding of their roles and responsibilities, and to obtain support for resources necessary to mitigate risks.

This presentation will be developed using Microsoft PowerPoint version 2003 (a later version may be used with the approval of the NRC).

**3.4 Monthly Report**

The Contractor shall provide a Monthly Performance Report that provides status of work accomplished, work forecast, and any concerns or potential problem areas. The format of the Monthly Performance Report must be agreed upon before work under this task order may begin. The Monthly Performance Report will be provided on the 5<sup>th</sup> of every month in Microsoft Word version 2003 format (a later version may be used with the approval of the NRC).

**4. Schedule**

One copy of each deliverable shall be provided electronically to the NRC. All report formats must be agreed to by the NRC before the reports are delivered. Deliverables shall be considered accepted by NRC if no edits have been sent to Contractor dated within one week of receiving each deliverable.

Description	Mode of Delivery	Due Date
Initial Project Plan; Kickoff Meeting	Onsite Meeting; Electronic submission and hard copies	5 calendar days after contract award
Monthly Status Report	Electronic submission and hard copies	5 <sup>th</sup> day of the month
Agency Mission Statement	Electronic submission	30 calendar days after contract award
Evaluation Criteria	Electronic submission	60 calendar days after contract award
Breakdown of Security Functions and Touch Points	Electronic submission	90 calendar days after contract award
Gap Analysis	Electronic submission	120 calendar days after contract award
Enterprise Risk Assessment Report	Electronic submission	150 calendar days after contract award
Documented Enterprise Risk Assessment Process	Electronic submission	180 calendar days following contract award

Description	Mode of Delivery	Due Date
Tools Report	Electronic submission	10 Days (Information Gathering Tools) 30 Days (Testing Tools)
Test Plan	Electronic submission	30 calendar days after contract award
Corrective Action Report	Electronic submission	60 calendar days after contract award
Presentation (Deliverable 6)	Onsite Meeting; Electronic submission (MS PowerPoint Document)	180 calendar days following contract award

#### 5. Period of Performance

The period of performance of this task order will be September 17, 2008 through September 16, 2009..

#### 6. Travel

A not-to-exceed (NTE) line item of \$20,00.00 has been included for travel that may be required for this effort. Trips will not be longer than a week in duration; travel and reimbursable expenses will be subject to appropriate government travel regulations; and the Contractor must obtain NRC approval prior to incurring any travel expense.

#### 7. Personnel

The Contractor shall assign a single individual to serve as the primary point of contact and project manager to support this task order. All Contractor personnel will be knowledgeable in one or more disciplines directly related to information. All personnel working on this task order must be pre-approved by the NRC.

Access to classified information is required. Since information protection is a very sensitive issue, Contractor personnel must have an approved background check that corresponds to the NRC information they need access too. It is anticipated that the Contractor will need an NRC "L" clearance.

#### 8. Meetings

The Contractor's Project Manager and technical representatives shall attend bi-weekly status meetings at NRC Headquarters to discuss work being done under this task order.