

ORDER FOR SUPPLIES OR SERVICES

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

BPA NO.

1. DATE OF ORDER SEP 25 2006		2. CONTRACT NO. (If any) GS35F0229K		6. SHIP TO:				
3. ORDER NO. DR-33-06-317-T007		4. REQUISITION/REFERENCE NO.		a. NAME OF CONSIGNEE U.S. Nuclear Regulatory Commission Attn: Carl Konzman				
5. ISSUING OFFICE (Address correspondence to) U.S. Nuclear Regulatory Commission Div. of Contracts Attn: CM33 Mail Stop T-7-I-2 Washington, DC 20555				b. STREET ADDRESS Mail Stop T-6-F-41 11545 Rockville Pike		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 SUITE 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/task 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 6-7N15-5H2357 N7235 252A 31X020 OBLIGATE: \$67,609.43				10. REQUISITIONING OFFICE OIS/BPIAD/ADMB				
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		
a. INSPECTION Rockville, MD	b. ACCEPTANCE Rockville, MD			9/24/2007		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)
	<p>TASK ORDER 7 UNDER NRC ORDER DR-33-06-317 (CISSS): The Contractor shall provide the U.S. Nuclear Regulatory Commission with, "Listed/Moderate Systems C&A: Budget Formulation Application (BFA)," services in accordance with the following:</p> <ul style="list-style-type: none"> - The attached Statement of Work - The attached Schedule of Supplies and Services and Prices - The terms and conditions of GSA Contract GS-35F-0229K - The terms and conditions of NRC Order DR-33-06-317 <p>Reference: MAR Quotation (Ref #2006-085/WA971), dtd 9/18/06</p> <p>DUNS: 062021639</p> <p>ACCEPTANCE: <i>Linda Klages</i> 9/21/2006 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.		\$67,609.43	17(h) TOTAL (Cont. pages) 17(i). GRAND TOTAL
	21. MAIL INVOICE TO:							
	a. NAME U.S. Nuclear Regulatory Commission Payment Team, Mail Stop T-7-I-2						\$67,609.43	
	b. STREET ADDRESS (or P.O. Box) Attn: DR-33-06-317-T007							
c. CITY Washington		d. STATE DC	e. ZIP CODE 20555					
22. UNITED STATES OF AMERICA BY (Signature) <i>Pew Lemell</i>					23. NAME (Typed) Eleni Jernell Contracting Officer TITLE: CONTRACTING/ORDERING OFFICER			

DELIVERY ORDER DR-33-06-317

TASK ORDER 7 (T007)

LISTED/MODERATE SYSTEMS C&A: BUDGET FORMULATION APPLICATION (BFA)

1.0 OBJECTIVE

The Contractor shall support the OIS in certification and accreditation of major information systems such that NRC is in compliance and maintains certification and accreditation currency with NIST and FISMA Guidance. The Contractor shall at a minimum develop associated certification and accreditation documentation consistent with the security support task referenced in SOW ENCLOSURE 6 of Delivery Order DR-33-06-317, entitled, "C&A PROCESS AND DELIVERABLES" such that an Authorization to Operate (ATO) which confers full accreditation shall be granted the system. The Contractor shall perform these security support tasks specified for a MODERATE security baseline systems.

The Contractor shall develop, at a minimum, the following information system security certification documentation: a security categorization, a risk assessment, a systems security plan, a security test and evaluation plan and associated report, a contingency test plan and report, and a plan of action and milestones to correct any identified deficiencies.

2.0 SCOPE OF WORK

The Contractor shall provide security analyst staff and develop all requisite systems certification and accreditation documentation such that the BFA system obtains an Authorization to Operate (ATO) and no system crosses fiscal year boundaries with an Interim Authorization to Operate (IATO).

System Name: Budget Formulation Application (BFA) – In Development

Sponsor Office: Office of the Chief Financial Officer (OCFO)

System Owner: Director, Office of the Chief Financial Officer (OCFO)

System Description: The purpose of the BFA system is to replace the legacy Controller Resource Database System (CRDS) in order to streamline the automation of the budget formulation process.

Status: BFA is currently operating under an interim approval to operate that expires on September 30, 2006. The status matrix below indicates the current (as of 8/15/06) BFA ISS C&A progress:

BFA Certification and Accreditation Status

	ATO/Expiration	Monthly Status Report (System Owner)	PIA (System Owner)	NRC FORM 616 (System Owner)	NRC FORM 637 (System Owner)	E-Authentication Risk Assessment	MOU (System Owner)	ISA (System Owner)	Security Categorization	C&A Schedule (System Owner)	Risk Assessment	System Security Plan	Corrective Action Plan	ATO Memo (System Owner)	SI & E Test Procedure Report	SI & E Test Procedure Execution Report	Contingency Plan Test Procedures Report	Contingency Plan Test Procedure Execution Report	
BFA (Listed) System Owner: OCFO	06/30/06	07/15/06	07/15/06	07/15/06	07/15/06	07/15/06	07/15/06	07/15/06	07/15/06	07/15/06	07/15/06	07/15/06	07/15/06	07/15/06	07/15/06	07/15/06	07/15/06	07/15/06	07/15/06
Completed (SIT/SC/DAA APPROVAL)	Package Submitted (PENDING SIT/SC/DAA APPROVAL)																		

The Contractor shall provide a security analyst staff and the development of the associated documentation associated with the security support tasks specified below for classified and unclassified LOW, MODERATE, and HIGH security baseline systems for the system category "Listed", as specified in SOW ENCLOSURE 6 of Delivery Order DR-33-06-317 - C&A PROCESS AND DELIVERABLES.

The term "Listed Application" means a computerized information system or application that processes sensitive information requiring additional security protections, and that may be important to the operations of an NRC office or region, but is not an MA when viewed from an agency perspective. Most NRC systems rely on the security protections provided by the NRC LAN/WAN GSS.

However, NRC offices have developed a number of additional non-major applications that are processing sensitive data such as individual privacy act information, law enforcement sensitive information, sensitive contractual and financial information, and other categories of sensitive information that the sponsor has determined will require additional security protections beyond the basic security provided by the NRC LAN/WAN. For those types of non-major applications that the sponsor has built in additional security protections and controls because of the added sensitivity of the information being processed, such a non-major application shall be categorized as a "Listed" System.

The security plan for a listed system will describe those additional security protections and controls. These additional security controls could refer to the use of additional passwords, or the use of additional security technology such as virtual private networks (VPNs), digital signatures, secure Web sites, or other security solutions based on the use of public key infrastructure (PKI) technology. In addition, any system that processes classified information or unclassified Safeguards Information (SGI) that is not a GSS or a MA shall be categorized as a Listed System. An abbreviated security plan format that is compliant with National Institute of Standards and Technology (NIST) security plan guidance is available on the NRC internal Web site.

3.0 PERIOD OF PERFORMANCE

The period of performance of this task order is September 25, 2006 through September 24, 2007.

4.0 FUNDING

- (a) The total estimated amount (ceiling) for the products/services ordered, delivered, and accepted under this task order is \$67,609.43.
- (b) The amount presently obligated with respect to this task order is **\$67,609.43**. 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 TRAVEL

No Travel is anticipated under this Task Order.

6.0 SCHEDULE

The Contractor shall provide final draft security documentation and reports for BFA consistent with the NRC-approved integrated project plan (Subtask 1).

7.0 SPECIFIC TASKS

The Contractor shall support the NRC C&A of BFA as described below:

Subtask 1: Integrated Security Activity Project Plan.

Develop and implement a project plan to ensure completion of the BFA certification and accreditation tasks within the period of performance. 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 project level (i.e., each system for which a certification and accreditation effort 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 can 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.

Subtask 2: Risk Assessment.

The assessment of risk and the development of system security plans are two important activities in an agency's information security program that directly support security accreditation and are required by the Federal Information System Management Act (FISMA) and OMB Circular A-130, Appendix III. Risk assessments influence the development of the security controls for information systems and generate much of the information needed for the associated system security plans.

The risk assessment shall characterize the information processed by using Federal Information Processing Standard (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems and National Institute of Standards and Technology (NIST) Special Publication (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 risk assessment shall be documented in a report that follows the NRC Template for Risk Assessment Report. The report shall be delivered in draft form and then in final form after NRC comments are incorporated. The NRC IT Security staff review of the draft is required to ensure compliance. The NRC Senior IT Security Officer must approve the final to enable system accreditation.

The Contractor shall track any residual risk in the plan of action and milestones (POA&M). The Contractor shall document the results of the 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 NRC and Contractor personnel to remediate all high and moderate security findings, and track the remaining security findings in the POA&M.

Subtask 3: Systems Security Plan (SSP).

The security plan 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 Contractor shall identify within the SSP the necessary security controls required, citing the security controls that are in place, those that are 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 system security plan shall be documented in a report that follows the NRC Template for System Security Plan. The report shall be delivered in draft form and then in pre-system ST&E form after NRC comments are incorporated. The NRC IT Security staff review of the draft is required to ensure compliance. The Contractor shall update the system security plan after completion of the ST&E test report to reflect validated in-place and planned controls. The NRC SITSO must approve the final to enable system accreditation.