

**AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT**

BPA NO. 1. CONTRACT ID CODE PAGE 1 OF PAGES 2

2. AMENDMENT/MODIFICATION NO. M002 3. EFFECTIVE DATE DEC 13 2007 4. REQUISITION/PURCHASE REQ. NO. OIS-06-317-71 5. PROJECT NO. (If applicable)

6. ISSUED BY CODE 3100 U.S. Nuclear Regulatory Commission Div. of Contracts Attn: Mail Stop T-7-I-2 Washington, DC 20555 7. ADMINISTERED BY (If other than Item 6) CODE 3100 U.S. Nuclear Regulatory Commission Div. of Contracts Mail Stop T-7-I-2 Washington, DC 20555

8. NAME AND ADDRESS OF CONTRACTOR (No., street, county, State and ZIP Code) MAR, INCORPORATED 1803 RESEARCH BLVD STE 204 ROCKVILLE MD 208506106 9A. AMENDMENT OF SOLICITATION NO. 9B. DATED (SEE ITEM 11) 10A. MODIFICATION OF CONTRACT/ORDER NO. GS35F0229K DR-33-06-317-T014 10B. DATED (SEE ITEM 13) 09-27-2006 CODE 062021639 FACILITY CODE X

**11. THIS ITEM ONLY APPLIES TO AMENDMENTS OF SOLICITATIONS**

The above numbered solicitation is amended as set forth in Item 14. The hour and date specified for receipt of Offers  is extended,  is not extended. Offers must acknowledge receipt of this amendment prior to the hour and date specified in the solicitation or as amended, by one of the following methods: (a) By completing Items 8 and 15, and returning \_\_\_\_\_ copies of the amendment; (b) By acknowledging receipt of this amendment on each copy of the offer submitted; or (c) By separate letter or telegram which includes a reference to the solicitation and amendment numbers. FAILURE OF YOUR ACKNOWLEDGMENT TO BE RECEIVED AT THE PLACE DESIGNATED FOR THE RECEIPT OF OFFERS PRIOR TO THE HOUR AND DATE SPECIFIED MAY RESULT IN REJECTION OF YOUR OFFER. If by virtue of this amendment you desire to change an offer already submitted, such change may be made by telegram or letter, provided each telegram or letter makes reference to the solicitation and this amendment, and is received prior to the opening hour and date specified.

12. ACCOUNTING AND APPROPRIATION DATA (If required) Not applicable.

**13. THIS ITEM APPLIES ONLY TO MODIFICATIONS OF CONTRACTS/ORDERS, IT MODIFIES THE CONTRACT/ORDER NO. AS DESCRIBED IN ITEM 14.**

(X) A. THIS CHANGE ORDER IS ISSUED PURSUANT TO: (Specify authority) THE CHANGES SET FORTH IN ITEM 14 ARE MADE IN THE CONTRACT ORDER NO. IN ITEM 10A. B. THE ABOVE NUMBERED CONTRACT/ORDER IS MODIFIED TO REFLECT THE ADMINISTRATIVE CHANGES (such as changes in paying office, appropriation date, etc.) SET FORTH IN ITEM 14, PURSUANT TO THE AUTHORITY OF FAR 43.103(b). C. THIS SUPPLEMENTAL AGREEMENT IS ENTERED INTO PURSUANT TO AUTHORITY OF: Mutual Agreement of the Parties. D. OTHER (Specify type of modification and authority)

**E. IMPORTANT:** Contractor  is not,  is required to sign this document and return <sup>2</sup> copies to the issuing office.

14. DESCRIPTION OF AMENDMENT/MODIFICATION (Organized by UCF section headings, including solicitation/contract subject matter where feasible.)

Please see page 2 for more information regarding this modification.

Reference: MAR Technical and Cost Proposal (Ref#: 2006-094/WA971), dated November 29, 2007.

Except as provided herein, all terms and conditions of the document referenced in Item 9A or 10A, as heretofore changed, remains unchanged and in full force and effect.

15A. NAME AND TITLE OF SIGNER (Type or print) Linda Klages UP, contracts 16A. NAME AND TITLE OF CONTRACTING OFFICER (Type or print) Eleni Jernell Contracting Officer 15B. CONTRACTOR/OFFEROR (Signature of person authorized to sign) 15C. DATE SIGNED 12-13-07 16B. UNITED STATES OF AMERICA BY (Signature of Contracting Officer) 16C. DATE SIGNED 12/10/07

The purpose of this modification is as follows:

- (1) To modify the Statement of Work to add the deliverable Subtask 6: Review, Verification, and Validation of Security Controls and Requirements.
- (2) To increase the ceiling amount by \$22,841.41 from \$111,374.04 to \$134,215.45.

Accordingly, the following changes are hereby made:

- (1) The Statement of Work is deleted in its entirety and replaced with the revised Statement of Work. The following sections of the Statement of Work have been revised:

- 1.0 OBJECTIVE
- 2.0 SCOPE OF WORK
- 4.0 FUNDING
- 7.0 SPECIFIC TASKS

- (2) The Schedule of Supplies or Services and Price/Cost is deleted in its entirety and replaced with the revised Schedule of Supplies or Services and Price/Cost.

This modification does not obligate any additional funds. All other terms and conditions remain unchanged.

Attachments: Revised Statement of Work  
Revised Cost Schedule

**DELIVERY ORDER DR-33-06-317  
TASK ORDER 14 (MOD 2)  
GENERAL SUPPORT SYSTEMS C&A: OPERATIONS CENTER INFORMATION  
MANAGEMENT SYSTEM (OCIMS)**

**1.0 OBJECTIVE**

The Contractor shall support the OIS in certification and accreditation of general support 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 HIGH security baseline systems.

The Contractor shall develop, at a minimum, the following information system security certification documentation: a Security Test and Evaluation (ST&E) plan and associated report, a Contingency Test Plan and report, and a Corrective Action Plan (CAP) to correct any identified deficiencies.

This task order is being modified to add Subtask 6: Review, Verification, and Validation of Security Controls and Requirements. This work is necessary because NSIR has recognized a need to update previously developed key security documents for the OCIMS system as a result of the ST&E phase of this task order.

**2.0 SCOPE OF WORK**

The Contractor shall provide security analyst staff and the development of all required systems certification and accreditation documentation associated with the security support tasks identified below for an unclassified HIGH security baseline system for the system category General Support System, and as specified in SOW ENCLOSURE 6 of Delivery Order DFt-33-06317 -C&A PROCESS AND DELIVERABLES such that the OCIMS obtains an Authorization to Operate (ATO)

**System Name:** Operations Center Information Management System (OCIMS)

**Sponsor Office:** Office of Nuclear Safety and Incident Response (NSIR)

**System Owner:** Director, NSIR

**System Description:** The Operations Center Information Management System (OCIMS) provides an integrated system comprised of three subsystems: Data, Display, and Voice. OCIMS is the primary means of creating, storing, sending, and retrieving information in the NRC's Operations Center.

**Status:** OCIMS is currently in production.

The Contractor shall provide 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 "General Support System", as specified in SOW ENCLOSURE 6 of Delivery Order DR-33-06317 -C&A PROCESS AND DELIVERABLES.

The term "General Support System" (GSS) is an interconnected set of information resources under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, and people (see Appendix III to OMS Circular No. A-130, "Security of Federal Automated Information Resources"). The mission objective of a GSS is to provide Automated Information System (AIS) resources in support of the organizational mission. Typical GSSs are LANs, WANs, servers, and data processing centers.

In order to meet the requirement NSIR requests to add a new subtask: Review, Verification, and Validation of Security Controls and Requirements. Schedule B, Item 4 Control Validation, identified activities to be performed and estimated cost.

### **3.0 PERIOD OF PERFORMANCE**

The period of performance of this task order is September 27, 2006 through January 31, 2008.

### **4.0 FUNDING**

(a) The total estimated amount (ceiling) for the products/services ordered, delivered, and accepted under this task order is **\$134,215.45**.

(b) The amount presently obligated with respect to this task order is **\$111,374.04**. 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 TRAVEL**

No travel is required.

### **6.0 SCHEDULE**

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

### **7.0 SPECIFIC TASKS**

The Contractor shall support the NRC C&A of the OCIMS system and application service provider facility as described below (including a ST&E plan and associated report, a Contingency Test Plan and report, and a Corrective Action Plan (CAP) to correct any identified deficiencies):

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

Develop and implement a project plan to ensure completion of the OCIMS 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: Systems Security Controls and Security Requirements Test Plan Development Support**

The Contractor shall support the NRC staff in the development and documentation of a test plan within the Rational Suite Enterprise that exercises the systems 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, 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 System Security Test and Evaluation Plan Template. The Contractor shall provide detailed test procedures to ensure all IT security functional and assurance requirements are fully tested. The procedures shall contain sufficient detail that a technically trained individual not familiar with the system can successfully follow the procedures.

The ST&E Plan shall identify all testing assumptions, constraints, and dependencies and include 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. 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 randomly individuals to verify that activities on the system follow the documented procedure or process as the activity is performed. (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 review and analyze visitor logs to verify all information requested has been entered on the log. (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 with the Contractor attempting to access a system by logging on to that system from his workstation (or other device) using an incorrect password to see if the system responds with an error message stating incorrect password or denies access after exceeding the maximum threshold for logon attempts and is directed to call the system administrator to gain access.

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 3: Review, Verification, and Validation of Security Controls and Requirements Test Plan and Test Plan Execution.**

The Contractor shall independently review, verify, and validate the security test plans and procedures to ensure the accuracy and adequacy of documented test procedures for all systems 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. The Contractor shall update the ST&E Plan after completion of the system security test and evaluation plan test report to

reflect validated information. The NRC Senior IT Security Officer must approve the final to enable system accreditation.

#### **Subtask 4: Contingency Plan.**

The Contractor shall support the NRC staff in the development and documentation of a contingency plan and test procedures within the Rational Suite Enterprise. The contingency plan shall be developed in accordance with NIST SP 800-34 Contingency Planning Guide for Information Technology Systems, NIST SP 800-37 Guide for the Security Certification and Accreditation of Federal Information Systems, and the NRC Contingency Plan (CP) Template. The Contractor shall provide detailed procedures for the notification and activation phase, recovery operations, and return to normal operations. The procedures shall contain sufficient detail that a technically trained individual not familiar with the system can successfully follow the procedures. The system contingency plan shall also contain sufficient personnel contact information to enable contact at all times, vendor contact information to enable contact at all times, equipment (hardware and software) and specification information to enable reconstitution of the system from scratch, all service level agreements and memoranda of understanding, the IT standard operating procedures for the system, identification of any systems that this system is dependent upon along with references for the applicable contingency plans, references to the emergency management plan and occupant evacuation plan, and references to the appropriate continuity of operations plan.

The system contingency plan shall be documented in a report that follows the NRC Template for System Contingency Plan. The report shall be delivered in draft form and then in pre-Test 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 contingency plan after completion of the contingency plan test report to reflect validated information. The NRC Senior IT Security Officer must approve the final to enable system accreditation.

#### **Subtask 5: Contingency Planning Test and Report.**

The Contractor shall provide expert advice and support during the Contingency Planning Test to ensure test plan documentation is compliant with the System Contingency Plan (CP) that has been approved by the NRC Senior Information Technology Security Officer (SITSO). Testing shall follow the test procedures developed and documented by the Contractor within the Rational Suite Enterprise. The Contractor shall document the testing in a System Contingency Test Report (CP Test Report). The CP Test Report shall be developed in accordance with NIST SP 800-34 Contingency Planning Guide for Information Technology Systems, NIST SP 800-37 Guide for the Security Certification and Accreditation of Federal Information Systems, and the NRC Contingency Test Report Template.

The CP Test shall be documented in a report that follows the NRC Template for the NRC Contingency Test Report. The CP Test Report shall identify all testing assumptions, constraints, and dependencies as well as any anomalies, impromptu tests, and deviations encountered during testing. The CP Test Report shall include the actual testing schedule and detailed test results for each test procedure outlining specific errors encountered. The CP Test Report shall include a table of test findings incorporating any test issues and recommendations. The CP Test Report shall identify any problems encountered during testing and identify the resulting action items for the system. The CP Test Report shall be delivered in draft form and then in final form after NRC comments are incorporated. The NRC

Senior Information Technology Security Officer (SITSO) must approve the final CP Test Report to enable system accreditation.

**Subtask 6: Review, Verification, and Validation of Security Controls and Requirements.**

The Contractor shall review, verify, and validate all 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. This subtask will permit MAR to update previously developed key security documents for the OCIMS system as a result of the ST&E phase. The documents to be updated are Risk Assessment and System Security Plan.