

2. AMENDMENT/MODIFICATION NO. M002	3. EFFECTIVE DATE See Block 16C.	4. REQUISITION/PURCHASE REQ. NO. OIS-06-317-37	5. PROJECT NO.(if applicable)
--	-------------------------------------	---	-------------------------------

6. ISSUED BY U.S. Nuclear Regulatory Commission Div. of Contracts Attn: CMB3 Mail Stop T-7-I-2 Washington, DC 20555	CODE 3100	7. ADMINISTERED BY (If other than Item 6) U.S. Nuclear Regulatory Commission Div. of Contracts Mail Stop T-7-I-2 Washington, DC 20555	CODE 3100
--	--------------	---	--------------

8. NAME AND ADDRESS OF CONTRACTOR (No., street, county, State and ZIP Code) MAR, INCORPORATED 1803 RESEARCH BLVD SUITE 204 ROCKVILLE MD 208506106	(X)	9A. AMENDMENT OF SOLICITATION NO.
		9B. DATED (SEE ITEM 11)
		10A. MODIFICATION OF CONTRACT/ORDER NO. GS35F0229K DR-33-06-317-T015
	X	10B. DATED (SEE ITEM 13) 09-27-2006

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).
X	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 ² (two) copies to the issuing office.

14. DESCRIPTION OF AMENDMENT/MODIFICATION (Organized by UCF section headings, including solicitation/contract subject matter where feasible.)
 The purpose of this modification is to revise the Statement of Work for Task Order 15 of DR-33-06-317 to both remove and add deliverables. In addition, this modification increases the Task Order ceiling by \$20,988.20 from \$99,657.34 to \$120,645.54.
 Reference: MAR Quotation (Ref# 2007-095/WA971), dated May 1, 2007
 This modification does not obligate any additional funds.
 Please see page 2 for more details on this modification.

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, Vice President, Contracts	16A. NAME AND TITLE OF CONTRACTING OFFICER (Type or print) Eleni Jernell Contracting Officer
15B. CONTRACTOR/OFFEROR <i>Linda Klages</i> (Signature of person authorized to sign)	15C. DATE SIGNED 05/04/2007
16B. UNITED STATES OF AMERICA BY <i>Eleni Jernell</i> (Signature of Contracting Officer)	16C. DATE SIGNED 5/3/07

The purpose of this modification is as follows:

- (1) To revise the Statement of Work to both remove and add deliverables.
- (2) To increase the ceiling amount by \$20,988.20 from \$99,657.34 to \$120,645.54.

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) In Section 4.0 FUNDING, paragraph (a) is deleted in its entirety and replaced with the following:

“(a) The total estimated amount (ceiling) for the products/services ordered, delivered, and accepted under this task order is **\$120,645.54.**”

ALL OTHER TERMS AND CONDITIONS REMAIN UNCHANGED

Attachments: Revised Statement of Work
Cost Schedule

**DELIVERY ORDER DR-33-06-317
TASK ORDER 15 (REVISED)
MAJOR/HIGH C&A: SECURE LOCAL AREA NETWORK/ELECTRONIC SAFE (SLES)**

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 HIGH security baseline systems.

The Contractor shall develop, at a minimum, the following information system security certification documentation: a security test and evaluation plan and the associated report for both the SGI-LAN system and the E-Safe systems that make up SLES.

2.0 SCOPE OF WORK

The Contractor shall provide security analyst staff and develop the system security control and security requirements test plan (ST&E procedures plan) and review, verification, and validation of security controls and requirements test plan and test plan execution (ST&E execution report) portion of the systems certification and accreditation relating to SGI-LAN and E-Safe.

System Name: Secure LAN and Electronic Safe System (SLES)

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

System Owner: Director, NSIR

System Description: The Secure Local Area Network/Electronic Safe (SLES) is a system for storage and retrieval of Safeguards Information (SGI). The digitized SGI material is placed into an electronic repository that does not have electronic connectivity to any other system and is located in a single controlled access room at Nuclear Regulatory Commission (NRC) Headquarters.

Status: SLES is presently under development.

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 "Major Application", as specified in SOW ENCLOSURE 6 of Delivery Order DR-33-06-317 - C&A PROCESS AND DELIVERABLES.

The term "Major Application" (MA) means a computerized information system or

application that requires special attention to security because of the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. Because of their impact on the agency mission and the information they contain or process, MA's require special management oversight. (See OMB Circular A-130, Appendix III.) For example, an agency wide financial management system containing NRC's official financial records would be an MA. A computer program or a spreadsheet designed to track expenditures against an office budget would not be considered an MA. Similarly, commercial off-the-shelf software products (such as word processing software, electronic mail software, utility software, or general purpose software) would not typically be considered MA's.

3.0 PERIOD OF PERFORMANCE

The period of performance of this task order is September 27, 2006 through September 26, 2007.

4.0 FUNDING

- (a) The total estimated amount (ceiling) for the products/services ordered, delivered, and accepted under this task order is **\$120,645.54**.
- (b) The amount presently obligated with respect to this task order is **\$99,657.34**. 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 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 SLES system and application service provider facility as described below:

Subtask 1: Integrated Security Activity Project Plan.

Develop and implement a project plan to ensure completion of the SLES 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 for the SGI-LAN and E-Safe systems that together comprise the SLES system.

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 SLES (SGI-LAN and E-Safe) 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 STE 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.