

| | | | | | |
|--|-----------|--|---|--------------------------------|-----------|
| AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT | | BPA NO. | 1. CONTRACT ID CODE | PAGE 1 | OF PAGE 3 |
| 2. AMENDMENT/MODIFICATION NO. M004 | | 3. EFFECTIVE DATE SEE BLOCK 15C. | 4. REQUISITION/PURCHASE REQ. NO. 33-06-317T045M004 DTD 4/9/2009 | 5. PROJECT NO. (if applicable) | |
| 6. ISSUED BY U.S. Nuclear Regulatory Commission Div. of Contracts Attn: Michele D. Sharpe Mail Stop: TWB-01-B10M Washington, DC 20555 | CODE 3100 | 7. ADMINISTERED BY (if other than Item 6) U.S. Nuclear Regulatory Commission Div. of Contracts Mail Stop: TWB-01-B10M Washington, DC 20555 | | CODE 3100 | |
| 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. GS35P0229K DR-33-06-317-T045 10B. DATED (SEE ITEM 13) 05-19-2008 | | |
| 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)
 B&R: 97S-15-5D1-328 JC: N7343 BOC: 252A
 APPN No.: 31X0200 FFS#: CS009309 OBLIGATE: \$250,000

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:
 D. OTHER (Specify type of modification and authority) Mutual Agreement Between Parties (reference is made to email agreement dated 5/7/2009)

E. IMPORTANT: Contractor ☐ is not, ☒ is required to sign this document and return ² copies to the issuing office.

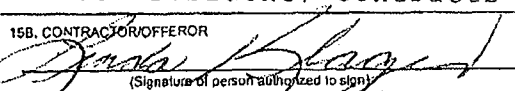
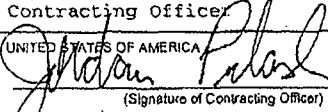
14. DESCRIPTION OF AMENDMENT/MODIFICATION (Organized by UCF section headings, including solicitation/contract subject matter where feasible.)

The purpose of this modification is to increase the level of effort (LOE) to perform annual testing on the listed systems, increase the not to exceed travel amount, provide incremental funding, and extend the period of performance.

Please see pages 2 through 3 for modification details.

This modification obligates FY 2009 funding in the amount of \$250,000.

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) Jordan Pulaski Contracting Officer | |
| 15B. CONTRACTOR/OFFEROR  (Signature of person authorized to sign) | 15C. DATE SIGNED 5-12-2009 | 16B. UNITED STATES OF AMERICA  (Signature of Contracting Officer) | 16C. DATE SIGNED 5-12-09 |

NSN 7540-01-152-8070
PREVIOUS EDITION NOT USABLE

STANDARD FORM 30 (REV. 10-83)
Prescribed by GSA - FAR (48 CFR) 53.243

TEMPLATE - ADM001

SUNSI REVIEW COMPLETE

MAY 15 2009

ADM002

The purpose of this modification is to increase the level of effort (LOE) to perform annual testing on the listed systems, increase the travel not to exceed amount, provide incremental funding, and extend the period of performance. The following is revised:

1. The Statement of Work (SOW) is revised to include the updated list of systems;
2. Increase the LOE by 2486 staff hours to perform annual testing on the 20 listed systems;
3. Increase the not to exceed travel (NTE) amount by \$11,445.56; thereby increasing the travel NTE from \$8,554.44 to \$20,000;
4. Increase the ceiling by \$308,167.41 (ceiling increase includes \$296,721.85 for testing of 20 systems and the additional travel amount of \$11,445.56); thereby increasing the ceiling from \$279,793.74 to \$587,961.15;
5. Provide incremental funding in the amount of \$250,000; thereby increasing the obligated amount from \$279,335.60 to \$529,335.60;
6. Extend the period of performance to December 31, 2009.

Accordingly, the following changes are hereby made:

1. The SOW is revised to update the list of systems (revised SOW attached).
2. Section 4.0 FUNDING 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 **\$587,961.15 (includes \$20,000.00 for NTE travel)**.
 - (b) The amount presently obligated with respect to this task order is **\$529,335.60**. 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.
3. SCHEDULE OF SUPPLIES OR SERVICES AND PRICE/COST is revised to include the following:

| SOW REF | DELIVERABLE TITLE AND REQUIRED LABOR CATEGORIES FOR COMPLETION OF DELIVERABLE FOR 1 SYSTEM | DISCOUNTED GSA LABOR RATE | HOURS FOR GSS SYSTEM | TOTAL AMOUNT FOR GSS SYSTEM | Discounted To (Per System) | | Total for 20 Systems | |
|---------|---|------------------------------|----------------------------|-----------------------------------|-------------------------------|---------|----------------------|---------|
| | | | | | Hours | Dollars | Hours | Dollars |
| | | | ONE SYSTEM | | | | | |
| 14 | Encl 6 | ANNUAL ANALYSIS | | | | | | |
| | Project Manager | \$ | | | | | 10,271.04 | |
| | QA Manager | \$ | | | | | 9,955.01 | |
| | Security Specialist II | \$ | | | | | 246,504.86 | |
| | Documentation Specialist | \$ | | | | | 17,471.48 | |
| | Technical Writer II | \$ | | | | | 12,519.36 | |
| | TOTALS FOR ANNUAL ANALYSIS | | | | | | 296,721.85 | |
| | | | | | Total \$ | | \$ 296,721.85 | |

| | |
|-----------------------------------|---------------------|
| TRAVEL COSTS | \$20,000 |
| TOTAL (Labor + NTE Travel) | \$587,961.15 |
| TASK ORDER CEILING | \$587,961.15 |

4. Section 3.0 PERIOD OF PERFORMANCE is deleted in its entirety and replaced with the following:

The period of performance for this task order is May 19, 2008 through December 31, 2009.

A summary of obligations from date of award through this action is given below:

| | |
|-------------------------------|----------------------|
| FY 2008 Obligated Amount..... | \$ 279,335.60 |
| FY 2009 Obligated Amount..... | <u>\$ 250,000.00</u> |
| Total Obligated Amount..... | \$ 529,335.60 |

This modification obligates FY 2009 funds in the amount of \$250,000.

U.S. Nuclear Regulatory Commission
Statement of Work for Task Order (45) Under DR-33-06-317
Annual Security Control Testing

1. Objective

The objective of this task order is to obtain professional services to support the Nuclear Regulatory Commission (NRC) in its annual information systems security control testing consistent with National Institute of Standards and Technology (NIST) Special Publication 800-53 Revision 2 and NIST SP 800-37. Specifically, the contractor shall assist NRC in performing required annual security control testing for NRC systems.

2. Background

The Federal Information Security Management Act (FISMA) of 2002 requires that each agency develop, document, and implement an agency wide information security program, approved by the Director under section 3543(a)(5), to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by (1) another agency, (2) contractor, or (3) other source, that includes – periodic assessments of the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency.

This activity will assist the NRC in ensuring adherence to federally mandated and NRC defined security requirements. Also, this activity will help the NRC to identify and understand the risks associated with operating these information systems.

For more information about annual control testing please see:

<http://csrc.nist.gov/publications/nistpubs/800-37/SP800-37-final.pdf> and
<http://csrc.nist.gov/publications/drafts/800-53A/draft-SP800-53A-fpd-sz.pdf>

3. Period of Performance

The period of performance for this task order is May 19, 2008 through December 31, 2009.

4. Funding

- (a) The total estimated amount (ceiling) for the products/services ordered, delivered, and accepted under this task order is **\$587,961. (includes \$20,000 for NTE travel)**.
- (b) The amount presently obligated with respect to this task order is **\$529,335.60**. 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.

U.S. Nuclear Regulatory Commission
Statement of Work for Task Order (45) Under DR-33-06-317
Annual Security Control Testing

5. Scope of Work

The Contractor shall provide all personnel, materials, hardware, software, labor, supplies, equipment, travel and other direct costs necessary to accomplish the performance of the activities described below to support the tasks specified in Statement of Work (SOW) Enclosure 6 of delivery Order DR-33-06-317 "Certification and Accreditation Process and Deliverables" for unclassified systems. If available, prior year self assessments and test results will be used as a reference, and tests performed under this task should leverage such previous work to the extent practicable.

Sponsor Office

NRC Computer Security Office (CSO)

System Owner

Multiple Offices in NRC (see Table 1 under Subtask 1 below).

System Description

All operational NRC major applications, general support systems, and contractor facilities identified in the NRC FISMA Inventory which have not been reviewed as part of a formal Security Test and Evaluation since August 15, 2007. Those systems that are planned to be tested under other tasks prior to August 15, 2008 should not be proposed under this task. Refer to Subtask 1, Table 1 for list of systems to be tested.

Instructions for Deliverables

Deliverables shall be consistent with period of performance in this statement of work and the detailed schedule required in Subtask 1. If for any reason a deliverable cannot be delivered within the specified time frame, the contractor shall notify the CSO (CSO project officer) in writing with cause and the proposed revised time frame. This notice shall include the impact on the overall project. The CSO shall make a business decision about the impact of the delay and forward the impact to the Contracting Officer.

Each deliverable shall first be submitted in draft for NRC review. NRC shall have 5 working days to review each draft deliverable and respond with comments or approval. If more time is required, the contractor will be notified in writing by the CSO. If revisions are required, the contractor has 3 days to complete the revisions and submit the revised draft deliverable to the CSO.

Once the deliverable is approved by CSO, the deliverable will become final. For each deliverable (draft or final), the contractor shall provide one (1) copy and one (1) electronic version of the deliverable to the CSO, unless otherwise indicated. All written deliverables shall be phrased in language that can be understood by the non-technical layperson. Statistical and other technical terms used in the deliverable shall be defined in a glossary.

U.S. Nuclear Regulatory Commission
Statement of Work for Task Order (45) Under DR-33-06-317
Annual Security Control Testing

All deliverables developed under this task order must be formatted in Microsoft Word, PowerPoint, or Excel (version 2003 or later version as approved by the CSO). Also, deliverables may be developed in PDF format. The templates used for each deliverable shall be developed by the contractor and approved by the CSO. Any changes to these templates must be approved by the CSO.

All deliverables and supporting documentation gathered or developed under this task order may not be stored on any device or piece of equipment that has not been approved by the CSO.

Schedule

The Contractor shall provide specific task deliverables consistent with the NRC-approved integrated project plan (Subtask 1). The period of performance is specified in Section 5.

6. Specific Tasks

Subtask 1: Integrated Security Activity Project Plan

Develop and implement a project plan to ensure completion of the Annual Security Control Test Reports within the period of performance (identified in Section 7 below). 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 system or site level (i.e., each system or site for which an Annual Security Control Test Report 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 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.

U.S. Nuclear Regulatory Commission
Statement of Work for Task Order (45) Under DR-33-06-317
Annual Security Control Testing

An updated high-level summary report detailing the current expected start and completion dates for each system's testing and deliverables shall be made available to the CSO upon request. The contractor shall keep CSO apprised of any actual or anticipated schedule delays or cost overruns.

Subtask 2: System and Control Selection

The contractor shall test the systems listed below. The contractor shall use the Annual Security Control Test report format used in FY08 testing (or other format suggested by the contractor and as approved by CSO) as the basis for each system's Annual Security Control Test Report.

1. ASLBP: DDMS
2. ASLBP: LSN
3. BPIAD: EIE
4. BPIAD: NSICD
5. BPAID: TAC
6. CFO: BFS
7. CFO: CAS
8. CFO: HRMS (Legacy)
9. HLW: CNWRA
10. ICOD: MPKI
11. ICOD: MAIL
12. IRSD: ADAMS
13. NMSS: GLTS
14. NRR: RPS
15. NSIR: E-SAFE
16. NSIR: SGI-LAN
17. SECY: EHD
18. Will be specified by the NRC Project Officer at a later date.
19. Will be specified by the NRC Project Officer at a later date.
20. Will be specified by the NRC Project Officer at a later date.

The contractor shall develop selection criteria to determine which controls will be tested in accordance with NIST SP 800-53 (see control CA-7), NIST SP 800-37 and OMB FISMA guidance. At a minimum, the selection criteria shall be based upon: the sensitivity level of the

U.S. Nuclear Regulatory Commission
Statement of Work for Task Order (45) Under DR-33-06-317
Annual Security Control Testing

system; the requirement to annually test volatile controls; controls called out for annual testing in OMB guidance; CSO specified controls; and those associated with system POAM items mark as "closed" since last control testing was performed. All other controls not tested under this task shall be planned to be tested at least once during the 3-year accreditation cycle. Upon selection criteria approval by the CSO, the contractor shall work with system owners and develop system specific plans for annual testing of controls (to include those tested under this task and those to be tested in subsequent years).

** Other Gov Systems only require verification/evidence of testing by sponsoring agency*

Subtask 3: Control Testing and Reporting

Based upon the test plans developed in Subtask 2, the Contractor shall perform a comprehensive assessment of the selected management, operational, and technical security controls of the systems identified in subtask 2 to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for each system consistent with NIST SP 800-53A. Prior to testing, the contractor shall hold a kickoff meeting with each system owner to review the scope of testing, controls selected, testing and documentation timeframes, required system owner support, and expected outcomes. Upon completion of testing the contractor shall develop Annual Security Control Test Report documentation for each system and incorporate any findings into each system's Plan of Action and Milestones (POAM).

Draft Annual Security Control Test Reports and the associated systems' POAM shall be submitted to the CSO for the purpose of coordination with the System owner. Upon System Owner review and comment, the contractor shall revise and update each Annual Security Control Test Report and POAM as appropriate and provide final versions to the CSO. A summary report shall be developed aggregating the findings across all systems. This summary Annual Security Control Test Report shall provide the CSO an overall view of the status of control implementation for all tested systems, as well as any observed vulnerability trends at an agency and system level with special attention to those deficiencies that would impact NRC FISMA compliance.

Subtask 4: Test Result Upload

Upon completion of Subtask 3, the contractor shall upload the test results and any resultant POAM action items into the CSO control tracking tool.

7. Travel

Travel may include trips to the 4 NRC Regional locations (listed below), the Technical Training Center (listed below), the CNWRA facility (listed below) and other government locations. Travel to each location shall be for 2 days and 1 night, for one security analyst. All travel, other than local travel, requires the prior approval of the NRC Project Officer. Travel costs should not exceed \$20,000 during this period of performance.

U.S. Nuclear Regulatory Commission
Statement of Work for Task Order (45) Under DR-33-06-317
Annual Security Control Testing

U.S. NRC Region I
475 Allendale Road
King of Prussia, PA 19406-1415

U.S. NRC Region II
Sam Nunn Atlanta Federal Center, 23 T85
61 Forsyth Street, SW
Atlanta, GA 30303-8931

U.S. NRC Region III
2443 Warrenville Road
Suite 210
Lisle, IL 60532-4352

U.S. NRC Region IV
Texas Health Resources Tower
611 Ryan Plaza, Suite 400
Arlington, TX 76011-4005

U.S. Nuclear Regulatory Commission
Technical Training Center
Osborne Office Center
5746 Marlin Road, Suite 200
Chattanooga, TN 37411-5677

Center for Nuclear Waste Regulatory Analyses (CNWRA)
Southwest Research Institute
6220 Culebra
San Antonio, TX 78228-0510

8. Meetings

The contractor's technical representative shall attend monthly status meetings at NRC Headquarters to discuss work being done under this task order.