

AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT

2. AMENDMENT/MODIFICATION NO. M003
 3. EFFECTIVE DATE SEE BLOCK 16C.
 4. REQUISITION/PURCHASE REQ. NO. 33-06-317T061M003
 5. PROJECT NO. (if applicable)

6. ISSUED BY CODE 310C
 U.S. Nuclear Regulatory Commission
 Div. of Contracts
 Attn: Jordan Pulaski
 Mail Stop: TWB-01-R10M
 Washington, DC 20555
 7. ADMINISTERED BY (If other than Item 6) CODE 310C
 U.S. Nuclear Regulatory Commission
 Div. of Contracts
 Mail Stop: TWB-01-R10M
 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
 CODE 062021639 FACILITY CODE
 9A. AMENDMENT OF SOLICITATION NO. (X)
 9B. DATED (SEE ITEM 11)
 10A. MODIFICATION OF CONTRACT/ORDER NO. GS35F0229K DR-33-06-317-T061
 10B. DATED (SEE ITEM 13) X 07-10-2009

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) N/A.

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) X Mutual Agreement.

E. IMPORTANT: Contractor is not, is required to sign this document and return 1 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 add IRDB to the list of developmental efforts, and to increase the ceiling by \$46,419.44 to \$171,734.21
 See the attached SOW and Price Schedule revisions that reflect these changes.

All other terms and conditions remain unchanged.

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. CONTRACTING OFFICER (Signature of person authorized to sign)
 15C. DATE SIGNED 9-17-2010
 16B. UNITED STATES OF AMERICA BY (Signature of Contracting Officer)
 16C. DATE SIGNED 9-20-10

Deliver Order DR-33-06-317
Task Order (61)
Computer Security Office (CSO)
Business Case Development

1.0 OBJECTIVE

The contractor shall provide support to the Nuclear Regulatory Commission (NRC) Computer Security Office (CSO) during design and development of information technology systems.

2.0 BACKGROUND

The NRC has mandated that the Project Management Methodology (PMM) outlined in Management Directive (MD) 2.8 will be used for the development of NRC Information Systems. MD 2.8 and its associated handbook are based on the Rational Unified Process (RUP) and include both the policy and configurable process with guidance, tools, and templates to support the implementation of an NRC information system.

The contractor must adhere to all the guidelines set forth in NRC's PMM process. The contractor shall use the IBM Rational Enterprise Suite of tools for data modeling, requirements management, test management, configuration management, and change management. Any proposed or actual deviation from the NRC PMM must be approved by the NRC Project Officer.

This task order is limited to the first two phases of the PMM process: Inception, and Elaboration.

The contractor will provide support for the following CSO development efforts:

- Information Assurance System (IAS) – Tier 2 Development Project
- Incident Response Database (IRDB)

IAS

The IAS system consists of several Commercial Off the Shelf (COTS) products loaded, tested and operated on a separate subnet that is capable of accessing the entire NRC infrastructure. The COTS products to be installed include but are not limited to: Encase, Hailstorm, Threatguard, and Secure Elements.

Each of these products provides a necessary automated Information Technology (IT) Security capability for the CSO. This suite of tools provides a real-time situational awareness capability to the members of the CSO Cyber Security Awareness (CSA) Team. The combination of these capabilities will enhance the mission of the CSA and allow it to perform its essential duties autonomously.

IRDB

The NRC IRDB will record and track incidents, help prevent future incidents, and support the overall incident response requirements of the NRC (including but not limited to the CSIRT and the NSIR Cyber Assessment Team). Recording and tracking Cyber incidents at a Federal agency is a requirement of FISMA. Currently, the NRC has no automated means of managing or reporting Cyber incidents. The IRDB will automate several time consuming internal processes and provide greater Cyber incident data consistency and accuracy. The data collected in the IRDB will also be a primary tool in managing a real-time situational awareness Cyber security posture at NRC. The IRDB will assist NRC in managing incidents to closure, and to share lessons learned through state-of-the-art software instead of paper-based, excel-based or verbal systems. The real-time accessibility to incident data is a key component as this will allow for valid and accurate incident metric reporting both internally (NRC executive management) and externally (FISMA, OMB, DHS).

3.0 SCOPE OF WORK

The contractor must provide support during the Inception and Elaboration phases of the NRC's PMM process. The contractor shall perform the following:

Tasks	IAS	IRDB
Subtask 1 – Integrated Project Pan	NA – Covered under Task Order 2.	NA – Covered under Task Order 71.
Subtask 2 – Requirements	The contractor shall develop the: As Is Model To Be Model System Requirements Specification (SRS) Vision Delivered Task Order Award +30 days	The contractor shall develop the Vision Delivered Task Order Award +30 days
Subtask 3 – Analysis, Design, Test, and Deployment	The contractor shall develop the System Architecture Document (SAD) Data Model Deployment Plan Test Plan Delivered Task Order Award +60 days	The contractor shall develop the System Architecture Document (SAD) Delivered Task Order Award +30 days

Tasks	IAS	IRDB
Subtask 4 – Project Management	The contractor shall develop the Screening Form CPIC Questionnaire Project Management Plan (PMP) Risk / Issues List Development Case Business Case Project Measures Records Management Form 637 Transmittal Memorandum Delivered Task Order Award +90 days	The contractor shall develop the Project Management Plan (PMP) Risk / Issues List Development Case E-Authentication Risk Assessment Security Categorization Privacy Impact Assessment Test Plan Records Management Form 637 Transmittal Memorandum Delivered Task Order Award +60 days
Subtask 5 – Certification and Accreditation Artifacts	NA – Covered under another task order	NA – Covered under another task order

The contractor shall provide the necessary security support staff to develop the associated documentation to support the tasks specified in SOW ENCLOSURE 6 of Delivery Order DR-33-06-317 "C&A PROCESS AND DELIVERABLES" for unclassified systems.

Note: The IRDB is a Tier 3 system. The contractor will be responsible for assisting the NRC with the PMM Capital Planning and Investment Control (CPIC) deliverables during the inception and elaboration phases of the project. If a deliverable is required by PMM but not listed above, the Contractor will assist the NRC in developing the appropriate documentation and procedures to satisfy PMM requirements. Only the System Security Plan has been excluded from this task order.

4.0 SCHEDULE

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

5.0 TASKS

The contractor shall support the Certification and Accreditation effort according to SOW Enclosure 6 and Section B "Schedule of Supplies or Services and Prices".

Note: Any Contractor personnel working under this task order can not take on the role of certification agent for any CSO system. At no time is the Contractor allowed to configure a CSO operational system. "Certification Agent" is defined as an individual, group, or organization responsible for conducting a security certification, or comprehensive assessment of the management, operational, and technical security

controls in an information system 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 the system. The certification agent also provides recommended corrective actions to reduce or eliminate vulnerabilities in the information system. Prior to initiating the security assessment activities that are a part of the certification process, the certification agent provides an independent assessment of the system security plan to ensure the plan provides a set of security controls for the information system that is adequate to meet all applicable security requirements.”

Subtask 1: Integrated Project Plan

The contractor shall develop and implement a project plan to ensure the completion of the tasks identified in this SOW occurs as expected. The contractor shall be required to develop and maintain an Integrated Security Activity Project Plan and perform Integrated Activity Scheduling. 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 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 Project Plan shall identify resources for each activity and include the Work Breakdown Structure levels. The Project Plan will include:

- **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.

- **Schedule and Budget**

The schedule and budget will identify what resources are needed, identify how much effort is required, and when each of the tasks specified in the WBS can be completed. 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: Requirements

The following Requirements documents shall be developed by the contractor during the execution of this task order

- **As Is Model** - Graphically describes an end-to-end sequence of activities grouped to demonstrate how a system is performing currently. The intent of this approach is to allow readers and reviewers to quickly achieve understanding and awareness regarding the current process.
- **To Be Model** - Graphically describes an end-to-end sequence of activities grouped to demonstrate how a system will perform once developed. The intent of this approach is to allow readers and reviewers to quickly achieve understanding and awareness on what the new system.
- **SRS** – Contains a collection of requirements for a system. For larger systems, the SRS should contain the collection of all requirements (including use cases and supplementary requirements) or RequisitePro requirements in a single document. For smaller systems, the SRS should contain all functional and non-functional requirements.
- **Vision** - This document helps collect, analyze and define high-level needs and features of a system under consideration for implementation. It focuses on the capabilities needed by the stakeholders and target users, and why these needs exist.

The contractor shall not consider subtask 2 complete until all Requirements Documents have been formally approved through the NRC CPIC process. The contractor shall make all necessary modifications to drafts to achieve this objective.

Subtask 3: Analysis, Design, Test, and Deployment

The following Analysis, Design, Test, and Deployment documents shall be developed by the contractor during the execution of this task order

- SAD - Provides a comprehensive architectural overview of the system, using a number of different architectural views to depict different aspects of the system. Views include Use-Case, Logical, Process, Deployment (physical), and Data. This is a high level design document.
- Data Model - Usually represented using an entity relationship diagram and data dictionary. The data model may include model elements for stored procedures, triggers, constraints, etc. that define the interaction of the application components with the database.
- Deployment Plan - Describes the set of tasks necessary to install and test the developed products such that they can be effectively transitioned. If the system will replace an existing system, compatibility, conversion, and migration issues must be addressed. Provides deployment sequence and schedule.
- Test Plan – Details the goals and objectives of testing within the scope of the project, the items being targeted, the approach to be taken, the resources required, and the deliverables to be produced. Also includes the Test Cases and Scripts.

The contractor shall not consider subtask 3 complete until all Analysis, Design, Test, and Deployment Documents have been formally approved through the NRC CPIC process. The contractor shall make all necessary modifications to drafts to achieve this objective.

Subtask 4: Project Management

The following Project Management documents shall be developed by the contractor during the execution of this task order

- Screening Form
- CPIC Questionnaire
- Project Management Plan - Comprehensive, composite artifact that gathers all information required to manage the project. It encloses or refers to a number of artifacts (e.g. schedule, budget, QA Plan, CM Plan, Measurement Plan, Risk Management Plan, and Iteration Plans) and is maintained throughout the project. The level of detail may be tailored to match the project size and complexity.
- Risk / Issues List – Describes known and open risks to the project, sorted in decreasing order of importance and associated with specific mitigation or contingency actions. The Issues List provides the Project Manager with a way to record and track problems, exceptions, anomalies, or other incomplete tasks requiring attention that relate to the management of the project.
- Development Case - Describes the development process that you have chosen to follow in your project. The purpose of the Development Case is to capture the tailored process for the individual project. It serves as a qualifier for the development process configured for a project or an organization.
- Business Case (Combo + SSIV) (160 hours + SSIV 24 hours)
- Project Measurements - Project metrics such as earned value, quality, budgets, expenditures, defects, configuration management data, and other resource consumption as required by the project

management or the NRC leadership team should be collected and maintained by the project management team throughout the lifecycle of the project.

- Records Management Form 637 – Submitted to the NRC Records Officer (Chief, RFPSB, IRSD, OIS) to initiate a Records Management Assessment of the changes to system functionality or records related processes.
- Transmittal Memorandum

The contractor shall not consider subtask 4 complete until all Project Management Documents have been formally approved through the NRC CPIC process. The contractor shall make all necessary modifications to drafts to achieve this objective.

Subtask 5: Certification and Accreditation Artifacts

The following Certification and Accreditation Artifacts shall be developed by the contractor during the execution of this task order

- Security Categorization Package - Provides a common framework and understanding for expressing security that, for the federal government, promotes: (i) effective management and oversight of information security programs; (ii) consistent reporting to the Office of Management and Budget (OMB) and Congress on the adequacy and effectiveness of information security policies, procedures, and practices.
- E-Authentication Risk Assessment - Data collection vehicle for the e-Authentication Risk Assessment Report. The information requested in the questionnaire is derived from guidance provided by the OMB Memorandum M-04-04 and NIST Special Publication 800-63.
- Privacy Impact Assessment (PIA) - Assists agency management and staff in identifying and addressing information privacy when planning, developing, implementing, and operating agency electronic information and record-keeping systems that maintain information on individuals.
- Preliminary Security Risk Assessment (SRA) - Contains a detailed assessment of how the system satisfies the security control requirements.
- Preliminary System Security Plan (SSP) - Describes the information system and references key documents to support each in-place control (e.g. configuration management plan, incident response plan, security awareness and training plan, rules of behavior, system interconnection agreements).
- Preliminary Standards Test and Evaluation (ST&E) Plan - Guides security testing and evaluation of the security controls and provides important feedback to information system developers and integrators.
- Preliminary Contingency Plan (CP) - Emergency response plan, developed in conjunction with application owners and maintained at the primary and backup installation sites to ensure that a reasonable continuity of support is provided if events occur that could prevent normal operations. Contingency plans shall be routinely reviewed, updated, and tested to enable vital operations and resources to be restored as quickly as possible and to keep system downtime to a minimum. A Contingency Plan is synonymous with a disaster plan and an emergency plan. If the system/subsystem is to be located within a facility with an acceptable contingency plan, system-unique contingency requirements should be added as an annex to the existing facility contingency plan.

The contractor shall not consider subtask 5 complete until all Certification and Accreditation Artifacts have been formally approved through the NRC CPIC process. The contractor shall make all necessary modifications to drafts to achieve this objective.

6.0 PERIOD OF PERFORMANCE

The period of performance of this task order will be from July, 10 2009 through December 31, 2010.

7.0 FUNDING

- (a) The total estimated amount (ceiling) for the products/services ordered, delivered, and accepted under this task order is **\$171,734.21**.
- (b) The amount presently obligated with respect to this task order is **\$120,000.00**. 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.

8.0 TRAVEL

The following travel is required to support this effort:

- IAS – travel is not required for this effort.
- IRDB – travel is not required for this effort.

9.0 MEETINGS

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

