

## AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT

BPA NO.

1. CONTRACT ID CODE

PAGE 1 OF PAGE 2

2. AMENDMENT/MODIFICATION NO. M003		3. EFFECTIVE DATE SEE BLOCK 16C.	4. REQUISITION/PURCHASE REQ. NO. 33-06-317T013M003 DTD 10/28/2008		5. PROJECT NO. (If applicable)
6. ISSUED BY U.S. Nuclear Regulatory Commission Div. of Contracts Attn: 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  CODE 062021639			(X)	9A. AMENDMENT OF SOLICITATION NO.  9B. DATED (SEE ITEM 11)  10A. MODIFICATION OF CONTRACT/ORDER NO. GS35F0229K DR-33-06-317-T013  10B. DATED (SEE ITEM 13) 09-26-2006	
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) 610-15-5G1-344 D2413 252A 31X0200.610  
FFS# 10670875C DEOBLIGATE: -\$4.42

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:
X	D. OTHER (Specify type of modification and authority) Mutual Agreement Between Parties

E. IMPORTANT: Contractor ☐ is not, ☒ is required to sign this document and return <sup>3</sup> copies to the issuing office.

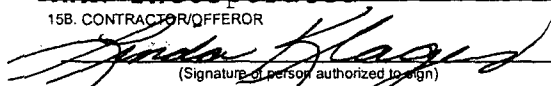
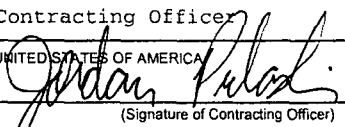
14. DESCRIPTION OF AMENDMENT/MODIFICATION (Organized by UCF section headings, including solicitation/contract subject matter where feasible.)

The purpose of this modification is to replace the PWPP system with the Akamai system

See page 2 for modification details.

This modification de-obligates FY 2006 funds in the amount of \$4.42. 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, VP Contracts MAR Incorporated		16A. NAME AND TITLE OF CONTRACTING OFFICER (Type or print) Jordan T. Pulaski Contracting Officer	
15B. CONTRACTOR/OFFEROR  (Signature of person authorized to sign)	15C. DATE SIGNED 1/15/2009	16B. UNITED STATES OF AMERICA BY  (Signature of Contracting Officer)	16C. DATE SIGNED 1-8-09

NSN 7540-01-152-8070

PREVIOUS EDITION NOT RELEASABLE

TEMPLATE - ADM001

SUNSI REVIEW COMPLETE

FEB 06 2009

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

ADM002

The purpose of this modification is to revise the Statement of Work to have the contractor perform the C&A of the Akamai system in place of the Public Website Production Platform (PWPP) system.

Accordingly the following revisions are hereby made:

1. The Statement of Work is replaced with the attached revised Statement of Work.
2. The ceiling and obligated amount is decreased by -\$4.42 thereby decreasing the ceiling and obligated amount from \$165,160.38 to \$165,155.96.

Thus, Section 4.0 "FUNDING" is revised to read as follows:

"(a) The total estimated amount (ceiling) for the products/services ordered, delivered, and accepted under this task order is \$165,155.96.

(b) The amount presently obligated with respect to this task order is **\$165,155.96.**"

3. The "SCHEDULE OF SUPPLIES OR SERVICES AND PRICE/COST" is deleted in its entirety and replaced with the following:

**SCHEDULE OF SUPPLIES OR SERVICES AND PRICE/COST**

**TASK ORDER 13 CEILING**

**\$165,155.96**

SOW REF	DELIVERABLE TITLE AND REQUIRED LABOR CATEGORIES FOR COMPLETION OF 1 DELIVERABLE FOR 1 SYSTEM	DISCOUNTED GSA LABOR RATE	HOURS FOR GSS SYSTEM	TOTAL AMOUNT FOR GSS SYSTEM	TO	
					Hours	Dollars
26	End 6 FULL C&A PACKAGE					
	Project Manager	\$				14,379.46
	QA Manager	\$				14,434.76
	Security Specialist III	\$				-
	Security Specialist II	\$				121,455.05
	Technical Writer II	\$				7,511.62
	Information Engineer	\$				-
	TOTALS FOR FULL C&A PACKAGE					157,780.88
4	8.0 CONTROL VALIDATION (ANNUAL)					
	Project Manager	\$				1,027.10
	QA Manager	\$				497.75
	Security Specialist III	\$				-
	Security Specialist II	\$				2,567.76
	Technical Writer II	\$				782.46
	TOTALS FOR CONTROL VALIDATION (ANNUAL)					4,875.07

Total \$ 162,655.96  
NTE Travel \$ 2,500.00  
Grand Total \$ 165,155.96

**DELIVERY ORDER DR-33-06-317**  
**TASK ORDER 13 (T013)**  
**CERTIFICATION AND ACCREDITATION OF AKAMAI**

**1.0 OBJECTIVE**

The Contractor shall support the Nuclear Regulatory Commission (NRC) in the Certification and Accreditation (C&A) of Akamai. The Contractor shall independently verify and validate Akamai is in compliance with federally mandated and NRC defined security requirements.

The Contractor shall at a minimum develop C&A 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".

The Contractor shall develop, at a minimum, the following information system security certification documentation:

- Security Categorization Package
- Risk Assessment
- Systems Security Plan
- Security Test & Evaluation (ST&E) Plan
- ST&E Execution Report
- Vulnerability Assessment Report
- Contingency Test Plan
- Contingency Test Report
- Plan of Action & Milestones Report

**2.0 SCOPE OF WORK**

The Contractor shall provide security analyst staff and develop all requisite C&A documentation for the Akamai system.

**System Name:** Akamai

**Sponsor Office:** Office of Information Services (OIS)/Information and Records Services Division (IRSD)

**System Owner:** Director, OIS/IRSD

**System Description:** Akamai delivers publicly available Web content from the NRC to users of the NRC Public Web Site. This service is provided through a proprietary network of over 20,000 computer servers positioned around the world. Requests for Web content are routed for optimal speed through the provider's network using a proprietary protocol. This service stores copies of requested content within the network so that requests can be fulfilled by the server nearest the requester. This service maintains a backup copy of the NRC web site so that requests for updated content can be first verified against that backup web site.

**Status:** Akamai is an application service provided by an offsite/non-NRC application service provider that will support the NRC in the development and delivery of publicly available NRC information as web content available through the Internet from NRC's external public web site.

The Contractor shall provide security analyst staff to develop the security documentation specified below for an unclassified General Support System. The system's sensitivity will be determined during the Security Categorization phase of the project. The security documentation will be developed as specified in SOW Enclosure 6 of Delivery Order DR-33-06-317 – C&A PROCESS AND DELIVERABLES.

### **3.0 PERIOD OF PERFORMANCE**

The period of performance of this task order is September 26, 2006 through June 30, 2009.

### **4.0 FUNDING**

- (a) The total estimated amount (ceiling) for the products/services ordered, delivered, and accepted under this task order is \$165,155.96.
- (b) The amount presently obligated with respect to this task order is **\$165,155.96**. 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**

Travel to the application service provider site is anticipated under this Task Order. A not-to-exceed (NTE) line item of \$2,500.00 has been included for travel required for this effort. All travel will be reimbursed in accordance with DR-33-06-317, Section 4.3, Travel Requirements.

### **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 Akamai 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 Akamai 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.

### **Subtask 4: Systems Security Controls and Security Requirements Support.**

The Contractor shall support the NRC staff in the development and documentation of security controls and security requirements and associated technical resolutions, risk mitigation, and implementations within the Rational Suite Enterprise.

### **Subtask 5: 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.

#### **Subtask 6: 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 7: Review, Verification, and Validation of Security Controls and Requirements Test Plan and Test Plan Execution.**

The Contractor shall independently review, verify, and validate all systems 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.

**Subtask 8: 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 9: 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 10: Quarterly Penetration and Vulnerability Scanning.**

The Contractor shall perform quarterly analysis, penetration, vulnerability, configuration, systems integrity, and patch management scans. The Contractor shall identify, analyze, and propose tested corrective actions that ensure the currency of the systems security posture and ensures that controls are operating as intended.

#### **Subtask 11: Annual Analysis of Systems Documentation, Security Controls, Requirements, and Implementation Status.**

The Contractor shall conduct on the Akamai system an inclusive independent audit annually that shall include but is not limited to the review, verification, and validation of all current systems documentation, analysis, penetration, vulnerability, configuration, systems integrity, and patch management scans. The Contractor shall identify, analyze, and propose tested corrective actions that ensure the currency of the systems security posture and ensures that controls are operating as intended. The Contractor shall identify NRC information systems security vulnerability trends at an agency and system level with special attention to those deficiencies that would impact NRC FISMA compliance.