

AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT		BPA NO.	1. CONTRACT ID CODE	PAGE 1
2. AMENDMENT/MODIFICATION NO. M018	3. EFFECTIVE DATE 07-27-2012	4. REQUISITION/PURCHASE REQ. NO. CSO-12-134 dte 5/22/12		5. PROJECT NO. (if applicable)
6. ISSUED BY U.S. Nuclear Regulatory Commission Div. of Contracts Attn: Wanda M Brown 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		(X)	9A. AMENDMENT OF SOLICITATION NO.	
CODE 062021639		9B. DATED (SEE ITEM 11)		
FACILITY CODE		10A. MODIFICATION OF CONTRACT/ORDER NO. GS35F0229K DR-33-06-317-T045		
		X	10B. DATED (SEE ITEM 13) 05-19-2008	

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) 2012-7S-51-J-145 N7343 252A 31x0200
 FFS# RQ122938 Obligate \$450,000.00
 NAICS 541511 PSC D313

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.
X	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) FAR 52.212-4 FAR-43.103(a)

E. IMPORTANT: Contractor is not, is required to sign this document and return 1 copies to the issuing office.

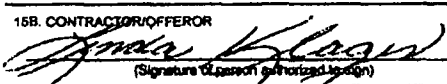
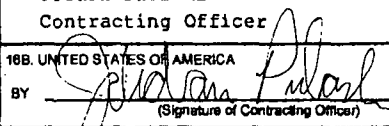
14. DESCRIPTION OF AMENDMENT/MODIFICATION (Organized by UCF section headings, including solicitation/contract subject matter where feasible.)
 The purpose of this modification is to (1) add additional work flow, (2) increase ceiling by \$650,000.00, (3) provide funding in the amount of \$450,000.00, and (4) extend the period of performance through 7/31/2013.

Please see page 2 for modification details.

Ceiling \$2,129,773.95 (changed)
 Total Obligations \$1,903,335.60 (changed)
 Period of Performance: 5/19/2008-7/31/2013 (changed)

The modification does obligate funds, all other terms and condition 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 of 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 7-24-12
16B. UNITED STATES OF AMERICA BY  (Signature of Contracting Officer)	16C. DATE SIGNED 7-25-12

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

JUL 30 2012

ADM002

The purpose of this modification is to (1) add within scope additional work flow in accordance with Statement of Work, (2) extend the period of performance from 10/31/2012 through 7/31/2013, (3) increase ceiling by **\$650,000.00** thereby increasing the ceiling amount from \$1,479,773.95 to **\$2,129,773.95**, and (4) provide funding in the amount of **\$450,000.00** thereby increasing the obligation amount from \$1,453,335.60 to **\$1,903,335.60**

Accordingly, the following changes are hereby made:

3.0 Period of Performance, 1st paragraph 2nd sentence is revised to read as follows:

The period of performance of this task order will be from date of award through July 31, 2013.

4.0 FUNDING, paragraph (b) 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 **\$2,129,773.95 (includes 40,000.00 for NTE Travel)**

(b) The amount presently obligated with respect to this task order is **\$1,903,335.60**

Accordingly, the following additions are hereby added under **Section 5.0 Scope of Work:**

5.0 Specific Tasks

Sub Task 5 Vulnerability Testing

Annual Security Controls and Vulnerability Test Plan

The contractor will develop a Annual Security Controls & Vulnerability Test Plan (ASC&VTP) that exercises the system's security controls and ensures those controls are operating as intended and have been implemented in accordance with federally mandated requirements / NRC defined surety requirements. The test plan will include elements from the ASCT and a hardening check that will be performed on the system. The results will provide an insight into whether the system's security controls are operating as intended.

The ASC&VTP contains sufficient detail that a technically trained individual not familiar with the system can successfully follow the procedures.

The following criteria shall be utilized during testing:

- **Examine** - The Contractor shall observe random individuals to verify that activities on the system follow the documented procedure or process as the activity are performed. For example, examine visitors upon computer room entry in order to verify that all visitation procedures are followed. The Contractor shall examine all processes, procedures, and documents associated with the system to ensure they are in compliance with established requirements.
- **Interview** - The Contractor shall interview personnel to verify the security policies and procedures are understood as implemented and prescribed by governing policies and regulations.
- **Inspection** - The Contractor shall ensure security controls have been properly implemented and maintained. For 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.
- **Test** - The Technical Test verification method shall be used to verify that each implemented control is functioning as intended. For example, the Contractor shall attempt to access the system by logging on to the system from an end user workstation (or other device) using an incorrect password to see if the system responds with an error message stating an incorrect password has been entered or denies access after exceeding the maximum threshold for logon attempts.

If a control is inherited, the Contractor shall review the inherited system's security documentation to determine if the control is in place and operating as intended. If it is not in place, this shall be factored in when the system's risks are determined.

If the control is not inherited, the Contractor shall ensure that the security control meets all federally mandated and NRC defined cyber security requirements and provides the appropriate level of protection based on the sensitivity of the system. This shall be determined through interviews, documentation reviews, or testing.

Security Control Testing

The system shall be reviewed, verified, and validated using the system's ASC&VTP and procedures to ensure the accuracy and adequacy of documented test procedures for all system security controls and associated technical resolutions, risk mitigation, and implementations contained within various NRC security and systems development documentation such that confirmation that the system and associated controls are operating as intended. Once testing has been completed, the ST&E Report, the Vulnerability Assessment Report, and the Plan of Actions and Milestones (POA&M) Report shall be developed to document the results. All findings that are not immediately remediated must be documented. All results will be documented in system's Security Risk Assessment (SRA) and System Security Plan (SSP).

A hardening check includes automated and manual testing of the different system platforms and applications to ensure security controls have been configured, operated, and maintained correctly. This shall be accomplished through interviews, documentation reviews, or testing depending on the security control being assessed. The expected sample for each system is:

- 30% of the system's components
- 2 of every type of device or server in each geographical location found in the system
- All devices or servers that are public facing must be tested

The Contractor shall be responsible for coordinating and executing all applicable site access, and authority to scan forms with other parties for the commencement of the above mentioned activities.

Examples of some of the standards that must be checked:

- National Institute of Standards and Technology (NIST) Federal Information Processing (FIPS) 140-2. When checking NIST FIPS 140-2, the Contractor must ensure that all cryptography used in the system has been validated, has a current FIPS 140-2 certificate, and the configuration of that cryptography complies with the security policy specified by the certificate for the cryptographic module.
- NIST 800-53A. The Contractor must ensure the system complies with the technical, managerial, and operational | controls found in this standard.
- NRC Cyber Security Standards. NRC Cyber Security standards ensure a consistent application of security across NRC information systems and provide a minimally acceptable level of security for devices, operating systems and applications. **NRC Cyber Security Standards are used as system baseline configurations for any information system that stores, transmits/receives, or processes NRC information.**

Please note: Individual Contractors working with the system owner to develop the system's E-Authentication Risk Assessment, Security Categorization Package, or SSP cannot be involved in system testing. This would be considered a conflict of interest.

Vulnerability Test (VT) for the following systems:

- EIG – small system -
- T&L Modernization - small system -
- LTS - small system -
- Telecom - moderately sized system -
- EPM - moderately sized system -
- SLES – large system -
- BASS – large system -
- ADAMS – large system -
- DCS – infrastructure system -
- ITI – infrastructure system -

(1) The schedule of supplies or Services is deleted in its entirety and replaced with the following:

See spreadsheet next page....

DR-33-06-317T04

6-7

MOD 18

A summary of obligations for this delivery order from award date through the date of this action is given below:

FY'08 Obligation Amount	-----	\$279,335.60
FY'09 Obligation Amount	-----	\$575,000.00
FY'10 Obligation Amount	-----	\$ 15,000.00
FY'11 Obligation Amount	-----	\$314,000.00
FY'12 Obligation Amount	-----	<u>\$ 720,000.00</u>

Cumulative total of NRC obligations is: **\$1,903,335.60**

This modification does obligates FY12 funds in the amount of \$450,000.00; all other terms and conditions under this contract task order remain unchanged.