

AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT

BPA NO.
GS35F0229K

1. CONTRACT ID CODE

PAGE 1 OF 9

2. AMENDMENT/MODIFICATION NO. M037
 3. EFFECTIVE DATE 11-02-2012
 4. REQUISITION/PURCHASE REQ. NO. CSO-13-002
 5. PROJECT NO. (If applicable) 10/1/12

6. ISSUED BY CODE 3100
 U.S. Nuclear Regulatory Commission
 Div. of Contracts
 Attn: Wanda M Brown
 Mail Stop: TWB-01-B10M
 Washington, DC 20555
 7. ADMINISTERED BY (If other than Item 6) CODE 3100
 U.S. Nuclear Regulatory Commission
 Div. of Contracts
 Mail Stop: TWB-01-B10M
 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.
 9B. DATED (SEE ITEM 11)
 10A. MODIFICATION OF CONTRACT/ORDER NO. GS35F0229K DR-33-06-317-T071
 10B. DATED (SEE ITEM 13) 08-31-2009

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) 2013-7S-51-J-145 N7343 252A 31x0200
 FFS# Obligate
 NAICS 541511

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: FAR 52.212-4
 D. OTHER (Specify type of modification and authority)

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) exercise a within scope change to the SOW by adding Task 6.0 Automated Scanning Capability, (2) decrease Labor category funding by \$131,541.62, and (3) increase ODC funding by \$131,538.81
 See page 2 for modification details

Ceiling \$8,335,111.40 (unchanged)
 Total Obligation Amount \$6,521,302.00 (unchanged)
 Period of Performance 9/16/2009-7/31/13 (unchanged)
 This modification does not obligate funds; all other conditions remaining 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
 15B. CONTRACTOR/OFFEROR (Signature of person authorized to sign)
 16A. NAME AND TITLE OF CONTRACTING OFFICER (Type or print) Wanda M Brown Contracting Officer
 16B. UNITED STATES OF AMERICA BY (Signature of Contracting Officer)
 16C. DATE SIGNED 10-31-12
 16C. DATE SIGNED 11-1-12

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

NOV 1 2012

ADM002

The purpose of this modification is to exercise a within scope change in accordance to FAR 52.212-4 by adding Task 6.0 Automated Scanning Capability and decrease funding from Category-Labor by \$131,541.62 from \$8,169,144.21 to \$8,037,572.59, and increase funding to Category-Other Direct Cost by \$131,538.81; increasing the ODC category from \$126,000.00 to \$257,538.81.

Accordingly, the following changes are hereby incorporated:

6.0 Task: Automated Scanning Capability

Purpose:

On task order DR330631771, a firm fixed price ODC that will be used to support an initiative to employ an automated scanning capability that can assess NRC information technology components against approved NRC configuration management baselines.

Objective/Deliverables:

1. The ODC will be broken into 4 different phases. The first two phases will be executed when the modification is first established. The other two phases will be executed as options as the project progresses.
2. The phases for the initiative are
 - a. Phase 1 –Contractor will conduct a Best Practice/Configuration Review of the NRC's nCircle implementation and will provide configuration changes that should be made to more effectively use the tool.
 - b. Phase 2 – Contractor will develop two (2) templates that can be utilized with the NRC's nCircle implementation to assess NRC information technology resources in an automated fashion ensuring the resources address federally mandated and NRC defined cyber security requirements.
 - c. Phase 3 – Contractor will develop six (6) templates that can be utilized with the NRC's nCircle implementation to assess NRC information technology resources in an automated fashion ensuring the resources address federally mandated and NRC defined cyber security requirements.
 - d. Phase 4 – Contractor will develop six (6) templates that can be utilized with the NRC's nCircle implementation to assess NRC information technology resources in an automated fashion ensuring the resources address federally mandated and NRC defined cyber security requirements.

Phase Detail

The following describe each phase and identifies the services that the contractor is expected to provide.

Phase 1 – Perform Best Practices/Configuration Review (Required)

The Best Practices/Configuration Review includes the contractor's investigation of the implementation of the nCircle within the NRC environment, covering specific aspects of the configuration, reporting, management processes, and maintenance of the nCircle suite of tools. The review will investigate NRC's deployment from two major perspectives:

- Technology — the configuration of the software itself.
- Processes and Workflow — the scanning, reporting, and remediation lifecycle.

Technology

The contractor will use a combination of hands-on investigation, reviews of available process documentation, and interviews with key stakeholders to conduct the review. The contractor will carefully manage the level of detail to ensure all topics are addressed at least at a high level. The following are the standard topic areas that will be included in this review:

Topic Area	Task	Description
Configuration Auditing Program	Configuration Auditing Goals	Review NRC's goals and expectations for configuration auditing.
Operations	Ticket Review	Review status and resolution of all nCircle support tickets since the last tune up.
	Operational Issues	Review any outstanding issues as noted by NRC staff.
Architecture	Architecture Review	Review deployment of scan engines, management servers, and SQL databases and compare against best practices; suggest improvements as needed.
Network Profiles	Naming Conventions	Review naming conventions and structure for network profiles, asset groups, and meta-asset groups and compare to best practices; determine optimal settings for nCircle's Intelligence Hub if in use.
Asset Licensing	License Cleanup	Review licensed assets and recommend the removal of invalid or obsolete assets to free up license capacity.
Auto Grouping	Auto Group Configuration	Review configuration of auto-grouping and recommended improvements as needed.
Custom Properties	Custom Property Creation	Review custom properties against business needs and recommend improvements.

Topic Area	Task	Description
Port Profiles	Port Profile Configuration	Review port profiles in use and recommend ways to optimize discovery and performance.
Risk Levels	Risk Level Configuration	Review assigned risk levels and ensure they map to business needs.
Scan Credentials	Credentials Configuration	Review structure and use of credentials for scanning and compare to best practices.
Scan Engines	DNS Server Configuration	Review DNS settings and validate domain name resolution functionality.
Security	Audit Log Configuration	Review NRC's audit requirements and compare against audit log settings.
User Management	User and Roles Review	Review configuration of the nCircle users and roles, and the permissions granted; compare to best practices.
Software Upgrades	Current Version Installation	Review any issues or improvements delivered by newer versions of the nCircle product.
System Health	Health Events	Review any system health events.
Third Party Integration	Third Party Configuration	Review configuration of Checkpoint, NAC, HP CMDB, Remedy, and Vulnerability Scanner settings.
Scan Configuration	Discovery Ping Sweep Configuration	Review configuration of discovery ping sweeps including TCP SYN, ARP, etc. and compare against best practices.
	Port Scan Configuration	Review configuration of port scans including banner checking, OS socket usage, NMAP fingerprints, etc. and compare against best practices.
	Advanced Scan Configuration	Review configuration of advanced scan categories, including Antivirus settings, file monitoring for both Windows and UNIX, Oracle database instance configuration, Users configuration, etc. and compare against NRC's needs and best practices.
	Gather Host Information Configuration	Review configuration of host information gathering, including fingerprinting, NetBIOS probes, and DNS settings and compare against best practices.
	Web Content Scan Configuration	Review configuration of web content scanning, including paths, crawling, ports, and page depth, and compare against best practices.
Dashboard	Dashboard Configuration	Review configuration and operation of the nCircle's dashboard; validate settings and test NRC's implementation of the dashboard.
Compliance Policies	Compliance Policy Configuration	Review usage of nCircle policies and compare to best practice; suggest improvements or additional scanning based on typical peer group configurations.

Topic Area	Task	Description
	Custom Test Usage	Review design and functionality of custom tests implemented at the NRC.
	Create Policy From Asset Usage	Review NRC use of "Create Policy from Asset" capabilities; assist with the creation of policies from Gold Image systems as required.
Reports	Report Usage	Review NRC use of nCircle reports and compare to best practices.
Integration	External System Integration Proposals	Review capabilities for integration with external systems (ArcSight, Remedy, etc.)
Roadmap	Roadmap Presentation	Discuss future capabilities and estimated timeframes for future versions of the nCircle.
	Feature Requests	Document NRC feature requests and submit tickets for tracking and follow up.
Operations	Best Practice Recommendations	Review findings and provide documentation detailing what needs to be done.
Overall Tool Configuration	Assess the overall tool configuration	Determine if any tool configuration changes could be made to improve tool effectiveness

As the contractor identifies quick fix recommendations during the review, the contractor will document these changes and provide them to NRC. Most of the quick fix recommendations will fall into the category of tuning, i.e. adjustments to the nCircle configuration parameters that can be implemented very quickly. There will likely be other needed changes identified that will be longer range in scope, especially if these entail modifications to NRC's current processes and workflow.

Processes and Workflow

The contractor will review NRC's processes and workflow surrounding NRC's use of the nCircle and other tools that might be involved in remediation of vulnerabilities and compliance issues. This investigation covers key questions such as:

- Are current nCircle processes understood and followed?
- Will current nCircle processes be able to scale as the nCircle implementation is extended to other network segments and to include additional templates?
- What other impediments exist to achieving full nCircle deployment and how can these be mitigated?
- Is there significant manual effort that could be addressed through increased automation?

During the review, the contractor will work with NRC staff directly responsible for the day-to-day administration and management of the nCircle, to provide focused knowledge transfer on topics of interest or concern to NRC. During this knowledge transfer, the contractor will demonstrate and explore key concepts in the nCircle allowing for technical Q&A from NRC staff.

The contractor will conduct a technical debrief for NRC staff, covering the major findings and recommendations arising from the Best Practices/Configuration Review for the nCircle implementation. The contractor will discuss the modifications and optimization recommendations interactively with NRC.

The contractor will document all review findings and recommendations and will provide these to NRC in a narrative document, covering all the topic areas addressed during the review.

List of Deliverables

The contractor will provide the following Deliverable(s) to NRC during this phase:

DELIVERABLE	DESCRIPTION
Findings and Recommendations Report	Narrative document covering topic areas addressed during the configuration review and associated recommendations

Completion Criteria

The contractor will have fulfilled all of their responsibilities under this task upon NRC's acceptance of a final Findings and Recommendations Report.

Schedule and Work Location

The contractor will perform the review during a single visit to the NRC's offices in Rockville, MD. The schedule for the on-site portion of the review will be confirmed by mutual agreement between the contractor and NRC.

NRC Responsibilities

In order for the contractor to successfully perform the Services described in this task, the contractor requests the following from NRC:

1. Provide a conference room for meetings between the contractor staff and NRC staff
2. Provide adequate workspace facilities for contractor staff while working on site
3. Provide access to test and/or production implementations of nCircle.
4. Assign and engage review participants (subject matter experts) to work with the contractor to provide requirements and validate finding
5. Ensure some review participants are familiar with NRC's specific implementation of nCircle and can provide detailed technical information about NRC's current implementation of the tool and the networks being scanned.

Phase 2 – Develop two (2) nCircle Templates (Required)

The contractor will develop two (2) nCircle Templates that will be used in conjunction with the nCircle tool to assess NRC information technology resources in an automated fashion ensuring the resources address federally mandated and NRC defined cyber security requirements. NRC will provide the NRC defined cyber security requirements that must be incorporated into the nCircle templates.

The templates developed by the contractor must be approved by the NRC before they are considered complete.

The contractor will provide the following Deliverable(s) to NRC during this phase:

DELIVERABLE	DESCRIPTION
Develop two (2) nCircle templates that reflect NRC defined cyber security requirements	Templates that work with NRC's implementation of nCircle to assess implementation compliance against NRC specific cyber security requirements.

Phase 3 – Develop six (6) nCircle Templates (Optional)

The contractor will develop six (6) nCircle Templates that will be used in conjunction with the nCircle tool to assess NRC information technology resources in an automated fashion ensuring the resources address federally mandated and NRC defined cyber security requirements. NRC will provide the NRC defined cyber security requirements that must be incorporated into the nCircle templates.

The templates developed by the contractor must be approved by the NRC before they are considered complete.

The contractor will provide the following Deliverable(s) to NRC during this phase:

DELIVERABLE	DESCRIPTION
Develop six (6) nCircle templates that reflect NRC defined cyber security requirements	Templates that work with NRC's implementation of nCircle to assess implementation compliance against NRC specific cyber security requirements.

Phase 4 – Develop six (6) nCircle Templates (Optional)

The contractor will develop six (6) nCircle Templates that will be used in conjunction with the nCircle tool to assess NRC information technology resources in an automated fashion ensuring the resources address federally mandated and NRC defined cyber security requirements. NRC will provide the NRC defined cyber security requirements that must be incorporated into the nCircle templates.

The templates developed by the contractor must be approved by the NRC before they are considered complete.

The contractor will provide the following Deliverable(s) to NRC during this phase:

DELIVERABLE	DESCRIPTION
Develop six (6) nCircle templates that reflect NRC defined cyber security requirements	Templates that work with NRC's implementation of nCircle to assess implementation compliance against NRC specific cyber security requirements.
Develop six (6) nCircle templates that reflect NRC defined cyber security requirements	Templates that work with NRC's implementation of nCircle to assess implementation compliance against NRC specific cyber security requirements.

4.0. Funding

(a) The total estimated amount of this contract (ceiling) for the products/services ordered, delivered, and accepted under this contract is \$8,335,111.40 (includes \$40,00.00 for NTE Travel and NTE ODC **\$257,538.81**)

(b) The amount presently obligated with respect to this task order is **\$6,521,302.00**.

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

FY'09 Obligation Amount-----	\$ 755,205.00
FY'10 Obligation Amount-----	\$ 2,026,293.00
FY'11 Obligation Amount-----	\$ 1,565,946.00
FY'12 Obligation Amount-----	<u>\$ 2,173,858.00</u>
Cumulative total of NRC obligations is:	\$ 6,521,302.00

This modification does not obligate funds in. All other terms and conditions remain unchanged.
