AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT

BPA NO.	1. CONTRACT ID CODE	PAGE	OF PAGES
		1	3

2. AMENDMENT/MODIFICATION NO.	3. EFFECTIVE DATE	4. REQUISITION/PURCHASE REQ. NO.	5. PROJECT NO.(If applicable)
M002	See Block 16C.	33-06-317T041M002* FFS# 10970582	

6. ISSUED BY	CODE	7. ADMINISTERED BY (If other than Item 6)	CODE
U.S. Nuclear Regulatory Commission Div. of Contracts Attn: Michele D. Sharpe Mail Stop: TWB-01-B10M Washington, DC 20555	3100	U.S. Nuclear Regulatory Commission Div. of Contracts Mail Stop: TWB-01-B10M Washington, DC 20555	3100

8. NAME AND ADDRESS OF CONTRACTOR (No., street, county, State and ZIP Code)	(X)	9A. AMENDMENT OF SOLICITATION NO.
MAR, INCORPORATED 1803 RESEARCH BLVD STE 204 ROCKVILLE MD 208506106		9B. DATED (SEE ITEM 11)
		10A. MODIFICATION OF CONTRACT/ORDER NO. GS35F0229K DR-33-06-317-T041
CODE 062021639 FACILITY CODE	X	10B. DATED (SEE ITEM 13) 03-21-2008

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)

910-15-5E1-330 J1296 252A 31X0200.910
OBLIGATE: $1,000.00

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; authorization to proceed provided in email dated December 31, 2008

E. IMPORTANT: Contractor ☐ is not, ☒ is required to sign this document and return 3 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 remove and replace the WIS system with the ITI system at no additional cost to the government and provide incremental funding in the amount of $1,000.00, thereby increasing the obligated amount from $255,654.86 to $256,654.86.

See pages 2 through 3 for modification details.

This modification obligates FY 2009 funds in the amount of $1,000.00. 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)	16A. NAME AND TITLE OF CONTRACTING OFFICER (Type or print)
Linda Klages, VP Contracts MAR, Inc	Eleni Jernell Contracting Officer
15B. CONTRACTOR/OFFEROR Linda Klages (Signature of person authorized to sign)	15C. DATE SIGNED 2/4/2009
16B. UNITED STATES OF AMERICA BY Eleni Jernell (Signature of Contracting Officer)	16C. DATE SIGNED 2/18/09

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

TEMPLATE - ADM001

SUNSI REVIEW COMPLETE

FEB 23 2009

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

ADM002

The purpose of this modification is to replace the WIS system with the ITI system at no additional cost to the government and provide incremental funding in the amount of $1,000.00; thereby increasing the obligated amount from $255,654.86 to $256,654.86.

Accordingly, the following revisions are hereby made:

1. The Statement of Work is revised to replace the WIS system with the ITI system (attached).

2. SCHEDULE OF SUPPLIES OR SERVICES AND PRICE/COSTS is revised to read as follows:

Task Order Ceiling: $359,454.20

	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	ITI C&A		
				HIGH ONLY		Hours	Rate	Dollars
17	Encl 6	SECURITY CATEGORIZATION (1 SYSTEM)						
		Project Manager	$					$ 256.78
		QA Manager	$					$ 248.88
		Security Specialist IV						$ -
		Security Specialist III	$					$ 1,343.10
		Security Specialist II	$					$ 5,135.60
		Senior INFOSEC Engineer	$					$ -
		Technical Writer II	$					$ 1,001.60
		ALS FOR SECURITY CATEGORIZATION (1 SYS						**$ 7,985.96**
19	Encl 6	RISK ASSESSMENT (1 SYSTEM)						
		Project Manager	$					$ 1,540.68
		QA Manager	$					$ 1,493.28
		Security Specialist IV	$					$ -
		Security Specialist III	$					$ 7,521.36
		Security Specialist II	$					$ 47,247.52
		Senior INFOSEC Engineer	$					$ -
		Technical Writer II	$					$ 4,006.40
		TOTALS FOR RISK ASSESSMENT (1 SYSTEM)						**$ 61,809.24**
20	Encl 6	SYSTEM SECURITY PLAN (1 SYSTEM)						
		Project Manager	$					$ 1,027.12
		QA Manager	$					$ 995.52
		Security Specialist IV	$					$ -
		Security Specialist III	$					$ 5,372.40
		Security Specialist II	$					$ 20,542.40
		Senior INFOSEC Engineer	$					$ -
		Technical Writer II	$					$ 4,006.40
		TALS FOR SYSTEM SECURITY PLAN (1 SYSTE						**$ 31,943.84**
21	Encl 6	ST&E PROCEDURES PLAN (1 SYSTEM)						
		Project Manager	$					$ 1,027.12
		QA Manager	$					$ 995.52
		Security Specialist IV	$					$ -
		Security Specialist III	$					$ 1,074.48
		Security Specialist II	$					$ 20,542.40
		Senior INFOSEC Engineer	$					$ -
		Technical Writer II	$					$ 4,006.40
		TALS FOR ST&E PROCEDURES PLAN (1 SYST						**$ 27,645.92**

22	Encl 6	ST&E EXECUTION REPORT (1 SYSTEM)					
		Project Manager	$			$	1,027.12
		QA Manager	$			$	995.52
		Security Specialist IV	$		-	$	-
		Security Specialist III			-	$	2,148.96
		Security Specialist II				$	17,974.60
		Senior INFOSEC Engineer				$	-
		Technical Writer II				$	3,756.00
		Network Security Analyst	$			$	-
		TALS FOR ST&E EXECUTION REPORT (1 SYST				$	**25,902.20**
25	Encl 6	CORRECTIVE ACTION PLAN (1 SYSTEM)					
		Project Manager					513.56
		QA Manager					497.76
		Security Specialist IV	$		-	$	-
		Security Specialist III	$			$	5,372.40
		Security Specialist II	$			$	5,135.60
		Senior INFOSEC Engineer	$			$	-
		Technical Writer II	$			$	5,008.00
		Sr. Information Engineer	$			$	-
		'ALS FOR CORRECTIVE ACTION PLAN (1 SYST				$	**16,527.32**
25	Encl 6	FULL C&A PACKAGE (1 SYSTEM)					
		Project Manager	$			$	256.78
		QA Manager	$			$	248.88
		Security Specialist III	$			$	1,343.10
		Security Specialist II	$			$	2,567.80
		Senior INFOSEC Engineer	$			$	975.55
		Technical Writer II	$			$	1,001.60
		Sr. Information Engineer	$			$	-
		TOTALS FOR FULL C&A PACKAGE (1 SYSTEM)				$	**6,393.71**
4	Encl 6	*CONTROL VALIDATION (ANNUAL)*					
		Project Manager	$	0	$ -	$	513.56
		QA Manager	$	0	$ -	$	497.76
		Security Specialist III	$	0	$ -	$	5,372.40
		Security Specialist II	$	0	$ -	$	5,135.60
		Technical Writer II	$	0	$ -	$	5,008.00
		Sr. Information Engineer	$	0	$ -	$	-
		TOTALS FOR CONTROL VALIDATION (ANNUAL		0	$ -	$	**16,527.32**

3. Section 6.0 FUNDING is revised to read as follows:

"(a) The amount presently obligated with respect to this task order is **$256,654.86.**"

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

FY 2008 Obligation Amount.....$ 255,654.86
FY 2009 Obligation Amount.....$ 1,000.00
Total Cumulative Obligated Amount..... **$ 256,654.86**

This modification obligates FY 2009 funds in the amount of $1,000.00. All other terms and conditions remain unchanged.

DELIVERY ORDER DR-33-06-317

TASK ORDER NO. 41

Infrastructure Computer Operations Division (ICOD) Certification and Accreditation Support

1.0 OBJECTIVE

The contractor shall support the Computer Security Office (CSO) in the certification and accreditation of the following Office of Information Services (OIS) Infrastructure Computer Operations Division (ICOD) Automated Information Systems (AIS)

- Managed Public Key Infrastructure (MPKI) – General Support System – Sensitivity: Confidentiality (Moderate), Integrity (Moderate), and Availability (Moderate).
- Information Technology Infrastructure (ITI) – General Support System – Sensitivity: Confidentiality (High), Integrity (High), and Availability (Moderate)

2.0 BACKGROUND

The following summarizes the systems that the contractor will be working with:

MPKI

MPKI is an agency wide GSS in the Operational Phase of its life cycle. This GSS is undergoing a modification that includes seeking validation from the Federal Public Key Infrastructure Policy Authority (FPKIPA) and inclusion into the Federal Public Key Infrastructure hierarchy. MPKI provides services to generate cryptographic key pairs and certificate requests, issue digital certificates to subscribers, revoke digital certificates, and to back-up and restore private encryption keys where separate signature keys have also been issued. Through subscriber digital certificates, MPKI provides a means of proving identity in electronic transactions - much like a company badge or passport does in face-to-face interactions. The certificates also provide cryptographic keys for encrypting data.

The MPKI system includes two Certification Authorities (CA) both located in VeriSign's facility in Mountain View, California and a new subscriber identity verification process for external subscribers (Nuclear Regulatory Commission (NRC) business partners). The Certification Authorities are the NRC Internal Staff CA and the NRC External Partner CA. MPKI operates an internal enrollment service and a key escrow service for internal subscribers' private encryption keys. The CAs, the certificate revocation services, and authoritative certificate validation services are outsourced to a commercial Public Key Infrastructure (PKI) provider (VeriSign, Inc.), as called for in OMB M-05-05.

ITI

WIS provides services to the Nuclear Regulatory Commission (NRC) Information Technology (IT) infrastructure such as Windows directory authentication services, internal Domain Naming Services (DNS) resolution, Dynamic Host Configuration Protocol (DHCP) services, Web services utilizating Internet Information Server (IIS), and other applications hosted on the Microsoft Windows server platform.

All system components are connected through Local Area Network (LAN) / Wide Area Network (WAN) System using TCP/IP. The LAN/WAN System provides the interface between the WIS and other NRC systems. The following protocols are used within the WIS:

- Active Directory – LDAP (Lightweight Directory Access Protocol)

- DHCP
- DNS
- WINS – Windows Internet Name Services using NetBIOS (Network Basic Input/Output System) over TCP/IP
- IIS – Hypertext Transfer Protocol (http) and Hypertext Transfer Protocol over Secure Sockets Layer (https)
- SharePoint – RPC (Remote Procedure Call)
- LANDesk and Dell OpenManage – SNMP (Simple Network Management Protocol)

The ITI is used directly or indirectly by all NRC employees, contractors, and consultants. WIS does not currently use any non-Commercial Off the Shelf (COTS) software.

3.0 SCOPE OF WORK

The contractor must ensure the system has been installed, configured, and maintained according to federally mandated and Nuclear Regulatory Commission (NRC) defined security requirements. The contractor will identify any operational risks found that may affect the system's ability to perform its mission and protect its data (stored and transmitted). The contractor shall perform the following:

Tasks	MPKI	ITI
Subtask 2 - E-Authentication Risk Assessment	NA	NA
Subtask 3 - Security Categorization Package • Security Categorization Document • Security Categorization Memo • Privacy Impact Assessment • Records Management Form 637	Shall review the security categorization package, assist the system owner in updating package, and ensure the boundary of the system has been properly identified.	Shall review the Security Categorization Package, assist the system owner in updating package, and ensure the boundary of the system has been properly identified.
Subtask 4 - Security Risk Assessment (SRA)	Shall review and assist the system owner in updating the SRA	Shall develop the SRA.
Subtask 5 - System Security Plan (SSP)	Shall review and assist the system owner in updating the SSP	Shall develop the SSP
Subtask 6 - Preliminary System Testing	NA	Shall perform preliminary testing on the system that includes the system's information assurance controls and the system's technical controls. Testing will begin once the SSP is 50% complete. Technical controls will be done first.
Subtask 7 - Standard Test and Evaluation (ST&E) Plan	Shall develop ST&E Plan	Shall develop ST&E Plan.

Tasks	MPKI	ITI
Subtask 8 - System Testing • ST&E Report • Vulnerability Assessment Report • Corrective Action Plan	Shall perform system testing	Shall perform system testing on all system components.
Subtask 9 - Authority To Operate (ATO) Package • Approval to Operate Memo • Package Includes Named Deliverables	Shall put together an ATO Package for the system owner **The MPKI ATO package must be delivered to the system owner by May 9, 2008.**	Shall draft the ATO request memo and put together the ATO package for the system. The MPKI ATO Package must be delivered to the system owner by 4/1/2009.

The contractor shall ensure that the steps, templates, and reports outlining certification and accreditation in NRC's Project Management Methodology are utilized and followed.

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.

3.0 SCHEDULE

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

4.0 TASKS

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

Subtask 1: Integrated Security Activity 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: E-Authentication Risk Assessment

The contractor shall perform this task as identified in the table found in section 3 "Scope of Work".

Electronic authentication (e-authentication) is the process of establishing confidence in user identities electronically presented to an information system. The focus is on remote authentication of individual people over a network, for the purpose of electronic government or commerce. The OMB M-04-04 memorandum guidance applies to systems that have remote authentication of users of Federal agency information technology systems for the purposes of conducting Government business electronically (or e-government). The guidance does not apply to internal only systems or the authentication of servers, or other machines and network devices. NRC's policy is to only require separate E-authentication Risk Assessments on systems where it is required. E-Authentication Risk Assessments shall be consistent with OMB M04-04, NIST SP 800-30, NIST SP 800-60A, and NIST SP 800-63.

Subtask 3: Security Categorization Package

The contractor shall perform this task as identified in the table found in section 3 "Scope of Work".

Security categorization standards for information and information systems provide 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. NRC's Security Categorization Package contains the following deliverables: Security Categorization Memo, Security Categorization Document, Privacy Impact Assessment, and Records Management Form 637.

A Security Categorization Package shall be completed for each new major application/general support system, listed system, contractor system, and those owned by other Federal agencies.

Subtask 4: Security Risk Assessment

The contractor shall perform this task as identified in the table found in section 3 "Scope of Work".

This Assessment is an important activity in an agency's information security program that directly supports security accreditation and is required by the FISMA and OMB Circular A-130, Appendix III. This assessment influences the development of the security controls for an information system and generates much of the information needed for the system's security plan.

The assessment shall characterize the information processed by using FIPS 199, Standards for Security Categorization of Federal Information and Information Systems and NIST 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 assessment shall be documented in a report that follows the NRC Template for the Risk Assessment Report. The report shall be delivered in draft form and then in final form after NRC comments are incorporated.

Any residual risk is tracked in the Plan of Action and Milestones (POA&M) Report. The POA&M Report documents the results of this process. POA&Ms 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 to remediate all high and moderate security findings, and track the remaining security findings using the system's POA&M.Report.

Subtask 5: Systems Security Plan

The contractor shall perform this task as identified in the table found in section 3 "Scope of Work".

The SSP 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 SSP identifies the necessary security controls that are required, citing the security controls that are in place, those that are planned, those that are not 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 SSP shall be documented in a report that follows the NRC Template. The report shall be delivered in draft form and then in pre-system ST&E form after NRC comments are incorporated. The SSP shall be updated after completion of the ST&E test report to reflect validated in-place and planned controls.

Subtask 6: Preliminary Testing

The contractor shall perform a preliminary assessment of the system to ensure the system is compliant with federally mandated and NRC defined security requirements. The contractor shall identify any operational risks found that may affect the system's ability to perform its mission and protect its data (stored and transmitted). The contractor shall obtain from the system owner a list of deviations that have been approved by the Designated Approving Authorities (DAAs), so these risks can be factored in during testing. Accepted risks are still reported, evaluated, and documented.

This subtask includes the automated and manual testing of the different system platforms to ensure they have been configured, operated, and maintained correctly. Also, the contractor must ensure the entire system is

tested including those components not identified in this SOW. This testing specifically excludes any Development/Test Environment.

The following is a list 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 800-53 Rev 2 or later standard. The contractor must ensure the system complies with the technical, managerial, and procedural controls found in this standard.
- NRC Hardening Standards. The contractor must ensure the system meets all the NRC hardening standards. For a complete list of Hardening standards please see "http://www.internal.nrc.gov/ois/it-security/guidance.html".

  The CSO has purchased a Center for Internet Security License for the NRC giving the organization the ability to access CIS Benchmarks; to distribute CIS Benchmark documents and tools; and to use CIS Benchmarks for commercial purposes.

  Note: When a federally mandated configuration or NRC hardening standard have not been specified, the contractor will test that component using the vendor's suggested best security practices.

The contractor shall document the results and observations of this 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 the system owner to remediate all high/moderate security findings/risks and track those risks using a Plan of Action and Milestone (POA&M) Report.

The contractor shall be responsible for coordinating and executing all applicable site access and non-disclosure agreements and authority to scan forms with parties other than the Nuclear Regulatory Commission prior to commencement of the above mentioned activities, ensuring that project schedules are not impacted.

Subtask 7: ST&E Plan

The contractor shall perform this task as identified in the table found in section 3 "Scope of Work".

The ST&E plan exercises the system's 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 Guide for accessing the Security Controls in Federal Information Systems
- 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
- NRC System Security Test and Evaluation Plan Template

The ST&E plan provides detailed test procedures to ensure all federally mandated and NRC defined security requirements are fully tested. These procedures contain sufficient detail that a technically trained individual not familiar with the system can successfully follow the procedures.

The ST&E plan identifies all testing assumptions, constraints, and dependencies and includes 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. Also, the contractor shall ensure testing identifies any operational risks found that may affect the system's ability to

perform its mission and protect its data (stored and transmitted). Additionally, the contractor must ensure the ST&E Plan includes the entire 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 random individuals to verify that activities on the system follow the documented procedure or process as the activity is performed. For 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 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.
- **Technical Test** - The Technical Test verification method shall be used to verify that each implemented control is functioning as intended. For example, the contractor will 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.

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 8: System Testing

The contractor shall perform this task as identified in the table found in section 3 "Scope of Work".

The system shall be independently reviewed, verified, and validated using the system's security test plans and procedures to ensure the accuracy and adequacy of documented test procedures for all system 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. Once testing has been completed, the ST&E Report, the Vulnerability Assessment Report, and the Corrective Action Plan shall be developed to document the results of the system's testing. Finally, the ST&E Plan is updated to reflect validated information.

Subtask 9: ATO Package

The contractor shall perform this task as identified in the table found in section 3 "Scope of Work".

The ATO package documents the results of the system certification and provides the authorizing official with the essential information needed to make a credible risk-based decision on whether to authorize operation of the information system.

The ATO Package contains the following deliverables plus a corresponding CD that contains all supporting documentation: Security Categorization Document, SRA, SSP, ST&E Plan, ST&E Report, Vulnerability Assessment Report, Corrective Action Plan, and an Approval to Operate Request Memo.

All documentation must be provided to the CSO in both hard copy and electronically in MS Word. The SSP must be current (within 2 months). The SRA, ST&E Plan, ST&E Report, and VAR must be current (within 2 months).

5.0 PERIOD OF PERFORMANCE

The period of performance of this task order will be 12 months.

6.0 TRAVEL

The following travel is required to support this effort:

- MPKI - Mountain View, California (2 trips)
- ITI – Region IV (2 Trips)

7.0 MEETINGS

The contractor's technical representative shall attend monthly status meetings at NRC Headquarters to discuss work being done under this task order. For the MPKI System, the contractor's technical representative shall attend weekly status meetings at NRC Headquarters to discuss progress and the work being done.