

AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT		BPA NO.	1. CONTRACT ID CODE	PAGE 1	OF PAGES 3
2. AMENDMENT/MODIFICATION NO. M002	3. EFFECTIVE DATE SEE BLOCK 15C.	4. REQUISITION/PURCHASE REQ. NO. 33-06-317T037M002 FFS# 10970651C		5. PROJECT NO.(If applicable)	
6. ISSUED BY U.S. Nuclear Regulatory Commission Div. of Contracts Attn: Michele D. Sharpe 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			X	10A. MODIFICATION OF CONTRACT/ORDER NO. GS35F0229K DR-33-06-317-T037	
				10B. DATED (SEE ITEM 13) 09-27-2007	

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) B&R: 910-15-5G1-344 JC: D1418 BOC: 252A APPN: 31X0200.910
FFS# 10970651C OBLIGATE: \$27,287.07

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 (reference is made to email dated 5/4/2009)

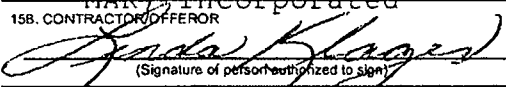
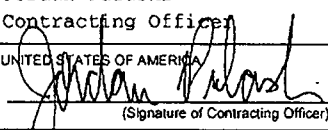
E. IMPORTANT: Contractor is not, is required to sign this document and return ² _____ copies to the issuing office.

14. DESCRIPTION OF AMENDMENT/MODIFICATION (Organized by UCF section headings, including solicitation/contract subject matter where feasible.)
The purpose of this modification is to increase the level of effort (LOE) and task order ceiling to enable the contractor to complete the C&A of the Voyager Integrated Library System (ILS).

Please see pages 2 through 3 for modification details.

This modification obligates FY 2009 funds in the amount of \$27,287.07.

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 MAR, Incorporated	15B. CONTRACTOR OFFEROR  (Signature of person authorized to sign)	15C. DATE SIGNED 5/11/2009	16A. NAME AND TITLE OF CONTRACTING OFFICER (Type or print) Jordan Pulaski Contracting Officer  (Signature of Contracting Officer)	16B. UNITED STATES OF AMERICA BY	16C. DATE SIGNED 5-7-09
---	---	-------------------------------	---	-------------------------------------	----------------------------

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

Aug 28 2009

ADM002

The purpose of this modification is to increase the level of effort (LOE) and increase the ceiling to enable the Contractor to complete the C&A of the Voyager Integrate Library System (ILS). The following is revised:

1. Statement of Work (SOW) is revised to incorporate additional Subtasks.
2. Increase the LOE by 258 staff hours;
3. Increase the ceiling by \$27,287.07; thereby increasing the ceiling from \$79,088.88 to \$106,375.95; and
4. Provide incremental funding in the amount of \$27,287.07; thereby increasing the obligated amount from \$79,088.88 to \$106,375.95.
5. Extend the period of performance to December 31, 2009.

Accordingly, the following revisions are hereby made:

1. Statement of Work (SOW) is revised to incorporate additional Subtasks (see attached revised SOW).
2. 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 **\$106,375.95**.

(b) The amount presently obligated with respect to this task order is **\$106,375.95**."

3. Section 3.0 PERIOD OF PERFORMANCE is revised to read as follows:

"The period of performance of this task order is September 27, 2007 through December 31, 2009."

4. SCHEDULE OF SUPPLIES AND/OR SERVICES is revised to include the following:

Sub-Task	SOW REF	DELIVERABLE TITLE AND REQUIRED LABOR CATEGORIES FOR COMPLETION OF 1 DELIVERABLE FOR 1 SYSTEM	DISCOUNTED GSA LABOR RATE	MOD 2 Pricing		
				Hours	Dollars	
3	17	Encl 6	SECURITY CATEGORIZATION (1 SYSTEM)			
		Project Manager	\$ 128.39	2	\$ 256.78	
		QA Manager	\$ 124.44	2	\$ 248.88	
		Security Specialist II	\$ 128.39	16	\$ 2,054.21	
		Technical Writer II	\$ 62.60	16	\$ 1,001.55	
		TOTALS FOR SECURITY CATEGORIZATION (1 SYSTEM)			36	\$ 3,561.41

4	19	Encl 6	RISK ASSESSMENT (1 SYSTEM)			
			Project Manager	\$		513.55
			QA Manager	\$		497.75
			Security Specialist II	\$		4,108.42
			Technical Writer II	\$		1,001.55
			TOTALS FOR RISK ASSESSMENT (1 SYSTEM)			6,121.27
5	20	Encl 6	SYSTEM SECURITY PLAN (1 SYSTEM)			
			Project Manager	\$		513.55
			QA Manager	\$		497.75
			Security Specialist II	\$		5,135.52
			Technical Writer II	\$		1,502.32
			TOTALS FOR SYSTEM SECURITY PLAN (1 SYSTEM)			7,649.15
8	22	Encl 6	ST&E EXECUTION REPORT (1 SYSTEM)			
			Project Manager	\$		256.78
			QA Manager	\$		-
			Security Specialist II	\$		5,135.52
			Technical Writer II	\$		1,001.55
			TOTALS FOR ST&E EXECUTION REPORT (1 SYSTEM)			6,393.84
9	26	Encl 6	FULL C&A PACKAGE (1 SYSTEM)			
			Project Manager	\$		256.78
			QA Manager	\$		248.88
			Security Specialist II	\$		2,054.21
			Technical Writer II	\$		1,001.55
			TOTALS FOR FULL C&A PACKAGE (1 SYSTEM)			3,561.41
			Totals			27,287.07

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

FY 2007 Obligated Amount.....	\$ 79,088.88
FY 2009 Obligated Amount.....	\$ <u>27,287.07</u>
Cumulative Obligated Amount.....	\$106,375.95

This modification obligates FY 2009 funds in the amount of \$27,287.07.

**DELIVERY ORDER DR-33-06-317
TASK ORDER 37**

LISTED/LOW SYSTEMS C&A: Technical Library Voyager Integrated Library System

1.0 OBJECTIVE

The Contractor shall support the OIS in certification and accreditation of a listed information system such that NRC is in compliance and maintains certification and accreditation currency with NIST and FISMA Guidance. The Contractor shall at a minimum develop associated certification and accreditation 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" such that an Authorization to Operate (ATO) which confers full accreditation shall be granted the system. The Contractor shall perform these security support tasks specified for a MODERATE security baseline system.

The Contractor shall develop, at a minimum, the following information system security certification documentation: an E-authentication risk assessment, a security categorization, a risk assessment and a systems security plan.

2.0 SCOPE OF WORK

The Contractor shall provide security analyst staff and develop all requisite systems certification and accreditation documentation such that the Voyager Integrated Library (ILS) obtains an Authorization to Operate (ATO).

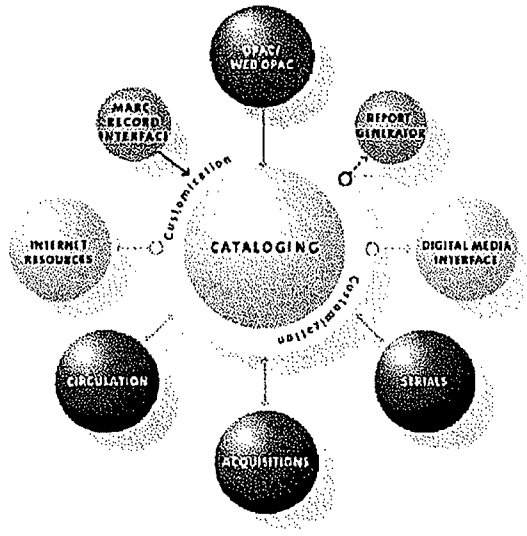
System Name: Voyager Integrated Library System (ILS)

Sponsor Office: Office of Information Services (OIS)

System Owner: Ed Baker, Director, OIS

System Description: Voyager is an integrated library system (ILS) developed by ExLibris Group. It is a commercial off-the-shelf (COTS) "product" and not an in-house system developed for NRC. The ILS is a software package used to perform the primary daily functions required for smooth and efficient library operations. The COTS software provides an automated approach to: cataloging new books and materials, circulation of items, serials management (checking in and routing journals), acquisitions, and searching of the online catalog (OPAC) for books, journals, or other materials for or by patrons.

The Voyager integrated library system (ILS) is a modular system. The primary module that serves as the centralized part of the system is the cataloging module. The cataloging module contains the bibliographic records (public records) which describe the material held in the library (by fields such as author, title, subject, and contents). The remaining modules of the system (e.g., serials, circulation, acquisitions, and the online catalog or OPAC) link over to the records in the cataloging module. In this way, a patron can pull up a bibliographic record in the online catalog, and see information on the item's circulating status (e.g., checked-out or in library), the order status (on order or received) and what issues have been received (if the item is a serial that is checked in). For a pictorial representation of the integrated system, please see the graphic below



The integrated library system has replaced former, and more manual methods of working in the library. It has replaced searching the holdings of a library by using the card catalog, replaced checking-in journals using a cardex system, replaced using paper check-out slips for circulating materials, and paper methods of ordering books and journals. It has automated all these functions into one system, that neatly integrates all aspects of the work and streamlines the processes required to do so.

Status: The Contractor shall provide security analyst staff to develop all requisite system certification and accreditation documentation such that the Voyager ILS obtains an Authorization to Operate (ATO).

Contractor shall provide a security analyst staff for the development of the associated documentation associated with the security support tasks specified below for unclassified LOW security baseline systems for the system category "Listed System", as specified in SOW ENCLOSURE 6 of Delivery Order DR-33-06-317, entitled, "C&A PROCESS AND DELIVERABLES".

OMB policy guidance requires that a security plan be in place for all sensitive systems. NRC uses the term Listed System to refer to a computerized information system or application that processes sensitive information requiring additional security protections, and that may be important to the operations of an NRC office or region, but is not an MA when viewed from an agency perspective. Most NRC systems rely on the security protections provided by the NRC LAN/WAN GSS. However, NRC offices have developed a number of additional non-major applications that are processing sensitive data such as individual privacy act information, law enforcement sensitive information, sensitive contractual and financial information, and other categories of sensitive information that the sponsor has determined will require additional security protections beyond the basic security provided by the NRC LAN/WAN. For those types of non-major applications that the sponsor has built in additional security protections and controls because of the added sensitivity of the information being processed, such a non-major application shall be categorized as a Listed System.

Tasks	Voyager (FY09 New Hardware)
Subtask 2 - E-Authentication Risk Assessment	N/A
Subtask 3 - Security Categorization Package	Shall update the Security Categorization Package
Subtask 4 - Security Risk Assessment (SRA)	Shall update the SRA
Subtask 5 - System Security Plan (SSP)	Shall update the SSP
Subtask 6 - Preliminary System Testing	N/A
Subtask 7 - Standard Test and Evaluation (ST&E) Plan	N/A
Subtask 8 - System Testing <ul style="list-style-type: none"> • Vulnerability Assessment Report • Plan of Action and Milestone (POA&M) Report 	Shall develop a VAR and POA&M Report.
Subtask 9 - Authority To Operate (ATO) Package <ul style="list-style-type: none"> • Approval to Operate Memo • Package Includes Named Deliverables • Includes a draft Security Assessment Report 	Shall put together an updated ATO Package for system owner.

3.0 PERIOD OF PERFORMANCE

The period of performance of this task order is September 27, 2007 through December 31, 2009.

4.0 FUNDING

- (a) The total estimated amount (ceiling) for the products/services ordered, delivered, and accepted under this task order is **\$106,375.95**.
- (b) The amount presently obligated with respect to this task order is **\$106,375.95**. 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 Office 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

No travel is required.

6.0 SCHEDULE

The Contractor shall provide final draft security documentation and reports for the Voyager ILS consistent with the NRC-approved integrated project plan (Subtask 1).

Subtask 1, the integrated security Activity Project Plan shall be delivered within one week of task order award.

7.0 SPECIFIC TASKS

The Contractor shall support the NRC C&A of Voyager ILS as described below:

Subtask 1: Integrated Security Activity Project Plan.

Develop and implement a project plan to ensure completion of the 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: E-Authentication Risk Assessment.

The Contractor shall conduct E-Authentication risk assessments and generate an E-Authentication risk assessment report consistent with OMB M04-04, NIST SP 800-30, NIST SP 800-60A, and NIST SP 800-63 as part of the security categorization.

Subtask 3: Security Categorization.

The Contractor shall conduct a security scoping interview to determine the proper system or applications classification and Impact consistent with NRC Management Directive 12.5, OMB Circular A-130, FIPS 199, and NIST Special Publication (SP) Series 800. Systems shall be categorized as Major Application, General Support System, Listed, or Other with a system impact of low, moderate, or high. The Contractor shall develop a systems security scoping report that identifies the system investment, system scope, inter-systems connectivity (diagram intersystem connections, data architecture, mapping, and data element definition and exchange between systems), the information sensitivity

levels of data processed within the system, the privacy impact of the system and whether it contains information in identifiable form (IFF), the electronic transactions (Inquire, Create, Delete, and Modify) and requisite authentication level, and electronic records disposition.

Subtask 4: 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 5: 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 6: Preliminary Testing

The contractor shall perform this task as identified in the table found in section 2 "Scope of Work".

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 2 "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 2 "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 2 "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.