

ORDER FOR SUPPLIES OR SERVICES

PAGE OF PAGES
1 90

IMPORTANT: Mark all packages and papers with contract and/or order numbers.

BPA NO.

1. DATE OF ORDER 28 7000		2. CONTRACT NO. (If any) GS-35F-0229K		6. SHIP TO:	
3. ORDER NO. DR-33-06-317		MODIFICATION NO.		4. REQUISITION/REFERENCE NO.	
5. ISSUING OFFICE (Address correspondence to) U.S. Nuclear Regulatory Commission Division of Contracts Two White Flint North - MS T-7-I-2 Washington DC 20555				a. NAME OF CONSIGNEE U.S. Nuclear Regulatory Commission	
				b. STREET ADDRESS Two White Flint North - MS T-6-C-30 Attn: Carl Konzman	
				c. CITY Washington	d. STATE DC
				e. ZIP CODE 20555	
7. TO:				f. SHIP VIA	
a. NAME OF CONTRACTOR MAR, INCORPORATED				b. TYPE OF ORDER	
b. COMPANY NAME				<input type="checkbox"/> a. PURCHASE <input type="checkbox"/> b. DELIVERY	
c. STREET ADDRESS 1803 RESEARCH BLVD STE 204				Reference your Please furnish the following on the terms and conditions specified on both sides of this order and on the attached sheet, if any, including delivery as indicated.	
d. CITY ROCKVILLE		e. STATE MD	f. ZIP CODE 208506106		
9. ACCOUNTING AND APPROPRIATION DATA Not Applicable. See Section B.6.				10. REQUISITIONING OFFICE OIS/BPIAD/ADMB	

11. BUSINESS CLASSIFICATION (Check appropriate box(es))				12. F.O.B. POINT N/A	
<input checked="" type="checkbox"/> a. SMALL	<input type="checkbox"/> b. OTHER THAN SMALL	<input type="checkbox"/> c. DISADVANTAGED	<input type="checkbox"/> d. WOMEN-OWNED	<input type="checkbox"/> e. HUBZone	<input type="checkbox"/> f. EMERGING SMALL BUSINESS
13. PLACE OF				14. GOVERNMENT B/L NO.	
a. INSPECTION	b. ACCEPTANCE			15. DELIVER TO F.O.B. POINT ON OR BEFORE (Date)	
				16. DISCOUNT TERMS N/A	

17. SCHEDULE (See reverse for Rejections)

ITEM NO. (A)	SUPPLIES OR SERVICES (B)	QUANTITY ORDERED (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)	QUANTITY ACCEPTED (G)
	<p>The Contractor shall provide the NRC with "Consolidated Information System Security Services (CISSS)," in accordance with the following: the SOW, Section B Schedule of Supplies or Services and Prices, the terms and conditions contained herein, and the terms and conditions of GSA Contract GS-35F-0229K.</p> <p>DUNS: 06-202-1639</p> <p>ACCEPTED:</p> <p><i>Linda Klages</i> MAR, Incorporated</p>					

18. SHIPPING POINT		19. GROSS SHIPPING WEIGHT		20. INVOICE NO.	
21. MAIL INVOICE TO:					
a. NAME U.S. Nuclear Regulatory Commission - CMB3					
b. STREET ADDRESS (or P.O. Box) Mail Stop T-7-I-2					
c. CITY Washington		d. STATE DC	e. ZIP CODE 20555		
SEE BILLING INSTRUCTIONS ON REVERSE					17(h) TOTAL (Cont. pages) \$10,578,135.07 17(i). GRAND TOTAL \$41,279,266.80

22. UNITED STATES OF AMERICA BY (Signature) <i>Eleni Jernell</i>	23. NAME (Typed) Eleni Jernell Contracting Officer TITLE. CONTRACTING/ORDERING OFFICER
--	---

AUTHORIZED FOR LOCAL REPRODUCTION
PREVIOUS EDITION NOT USABLE

SUNSI REVIEW COMPLETE

OPTIONAL FORM 347 (REV. 3/2005)
PRESCRIBED BY GSA/FAR 48 CFR 53.213(e)

TEMPLATE - ADM001

ADM002

B. SCHEDULE OF SUPPLIES OR SERVICES AND PRICES

Costs/prices listed in Section B and the referenced contract attachments reflect those proposed in "Part II, Final Revised Cost/Price Quote," submitted June 29, 2006 [MAR Proposal Number: 2006-044/WA971 REV], which is incorporated by reference. All labor categories, labor rates (and associated discounts), levels of effort, and other direct costs included in this quotation remain in full force and effect for the period of performance of this contract.

For contract performance, ceiling costs/prices for each single unit (this is for one (1) deliverable or one (1) annual service for one (1) system) are fixed by the system categorization type (major, GSS, listed, E-Gov, Other) and security baseline (high) for each year of the period of performance. The Contractor will be reimbursed for actual costs incurred only. The Contractor will not be permitted to exceed the fixed ceiling (unit cost) of a single unit or Task Order. Should actual costs not meet the fixed ceiling, then the Contractor will be reimbursed only for those actual costs and not for the fixed ceiling (unit cost) of the single unit or Task Order.

"Low" and "Moderate" *single unit* costs/prices (i.e., one (1) deliverable or one (1) annual service for one (1) system) for each system category (Major Applications, General Support Systems, Listed Systems, E-Government Systems, and Other Systems) will be negotiated prior to issuance of task orders. Single unit costs/prices for "Low" and "Moderate" systems are expected to result in lower single unit costs/prices (i.e., *an average percent difference of approximately 10-15%*, as stated in MAR's Proposal Number 2006-044/WA971 REV) than those incorporated into the contract for systems with a "High" security baseline. Task order quotations should utilize these single unit costs/prices for pricing the appropriate quantities of deliverables/effort proposed for each task order.

A summary of the contract amounts for the base year and option years is provided below:

CISSS CONTRACT VALUE INCLUDING OPTIONS	
BASE YEAR GRAND TOTAL	\$ 10,578,135.07
OPTION YEAR 1 GRAND TOTAL	\$ 8,668,650.35
OPTION YEAR 2 GRAND TOTAL	\$ 7,622,038.79
OPTION YEAR 3 GRAND TOTAL	\$ 7,434,765.90
OPTION YEAR 4 GRAND TOTAL	\$ 6,975,676.70
GRAND TOTAL (BASE + OPTION YEARS)	\$ 41,279,266.80

B.6 CONSIDERATION AND OBLIGATION

- (a) The total estimated amount of this contract (ceiling) for the products/services ordered, delivered, and accepted under this contract is \$10,578,135.07 (base period of performance). The Contracting Officer may unilaterally increase this amount as necessary for additional work with the contractor during the contract period provided the total contract value prescribed under this contract is not exceeded.
- (b) No funds are obligated on this order. Funds will be obligated on separate task orders, subject to the availability of funds.
- (c) The obligated amount(s) on the task orders may be unilaterally increased from time to time by the Contracting Officer by written modification. The total of the obligated amount(s) shall, at no time, exceed the contract ceiling as specified in paragraph (a) above. The total of the obligated amount(s) shall, at no time, exceed the ceiling specified in the task order. When and if the amount(s) paid and payable to the Contractor hereunder shall equal the obligated amount, the Contractor shall not be obligated to continue performance of the work unless and until the Contracting Officer shall increase the amount obligated with respect to this contract. Any work undertaken by the Contractor in excess of the obligated amount specified above is done so at the Contractor's sole risk.
- (d) The total amount of Option Year 1 for the products/services ordered, delivered, and accepted under this contract is \$ 8,668,650.35.
- (e) The total amount of Option Year 2 for the products/services ordered, delivered, and accepted under this contract is \$ 7,622,038.79.
- (f) The total amount of Option Year 3 for the products/services ordered, delivered, and accepted under this contract is \$ 7,434,765.90.
- (g) The total amount of Option Year 4 for the products/services ordered, delivered, and accepted under this contract is \$ 6,975,676.70.
- (h) The total amount of this Contract, including the Option Periods is \$41,279,266.80.

**SECTION C – STATEMENT OF WORK
U.S. NUCLEAR REGULATORY COMMISSION
CONSOLIDATED INFORMATION SYSTEM SECURITY SERVICES (CISSS)**

1.0 OBJECTIVE

The purpose of this contract is to obtain professional services to support the Nuclear Regulatory Commission (NRC) in its information systems security certification and accreditation process implementation. Presently, no unclassified NRC systems are fully accredited.

The Contractor shall develop security related documentation and perform the systems analyses required to obtain an Authorization to Operate (ATO) for national security, intelligence, and general information systems that will ensure cradle to grave compliance including: Federal Information Security Management Act (FISMA), Clinger-Cohen Act, Privacy Act of 1974, Financial Management Integrity Act, Financial Management Improvement Act, Federal Enterprise Architecture (FEA), Office of Management and Budget (OMB) M-04-04, OMB Circular A-123, Homeland Security Presidential Directive 7, Homeland Security Presidential Directive 12, OMB Circular A-130, OMB Circular A-11, National Security Directive 42, Executive Order 13356, Intelligence Reform and Terrorism Prevention Act, Director of Central Intelligence Directive 6-1, Director of Central Intelligence Directive 6-3, Director of Central Intelligence Directive 6-5, Director of Central Intelligence Directive 8-1, Federal Information Processing Standard (FIPS) 199, Federal Information Processing Standard 201, Federal Information Processing Standard 200, NIST 800 Series, National Strategy for Secure Cyberspace, OMB Information System Security Line of Business, and other applicable OMB and National Institute of Standards and Technology (NIST) series security certification and accreditation requirements for classified and unclassified information systems.

Furthermore, it is the intent of the Office of Information Services (OIS) to implement an Information Systems Security (ISS) services contract which integrates with the Enterprise Architecture and Capital Planning and Investment Control (CPIC) process. The ISS program, Enterprise Architecture, and the CPIC process mandate how IT dollars are spent relative to return on investment, and ensure corporate compliance and fiscally responsible IT investment management through close integration and support of OMB Exhibit 300 and 53 submissions. The Contractor shall implement an integrated approach to security services that supports improved mission support, IT investment management, and consistent and repeatable service delivery in the Security Certification and Accreditation with ATO for all NRC IT systems.

2.0 CONTRACT TYPE

This is an IDIQ time and materials (T&M) with a fixed ceiling, task order contract. For contract performance, ceiling costs/prices for each single unit (this is for one (1) deliverable or one (1) annual service for one (1) system) are fixed by the system categorization type (major, GSS, listed, E-Gov, Other) and security baseline (high) for each year of the period of performance. The Contractor will be reimbursed for actual costs incurred only. The Contractor will not be permitted to exceed the fixed ceiling (unit cost) of a single unit or Task Order. Should actual costs not meet the fixed ceiling, then the Contractor will be reimbursed only for those actual costs and not for the fixed ceiling (unit cost) of the single unit or Task Order.

3.0 SCOPE

The Contractor shall provide all personnel, materials, hardware, software, labor, supplies, equipment, travel and other direct costs necessary to accomplish the performance of the tasks described below. This contract will be accomplished through the issuance of task orders.

4.0 PERIOD OF PERFORMANCE

The base period of performance is **July 31, 2006 through July 30, 2007**. There are four option periods of performance. Each option year period of performance is twelve (12) months. **Note:** Any work beyond February 9, 2010 is subject to exercise of the optional period of performance under GSA contract GS-35F-0229K (reference Section C.24, OPTION TO EXTEND THE TERM OF THE CONTRACT). However, should GSA exercise this option, all pricing and rates in this contract will remain in full force and effect. New task orders will not be issued beyond February 9, 2010 until and unless the option is exercised under GSA contract GS-35F-0229K.

4.1 Hours of Operation

The Contractor shall have access to the Government facilities: five (5) days per week, Monday through Friday from 7:00 a.m. to 4:30 p.m., except when the Government facility is closed due to local or national emergencies, administrative closings, or similar Government directed facility closings.

4.2 Place of Performance

For all unclassified efforts, the primary place of performance shall be at the Contractor's facility. The Contractor facility, off-site services, or telecommuting locations shall be located within the continental United States (CONUS). The Contractor shall have broadband access and computers for all personnel. Any classified work shall be performed on-site at NRC facilities.

4.3 Travel Requirements

- (a) Occasional travel to the NRC Headquarters located in Rockville, Maryland shall be required. Local travel expenses will not be reimbursed by the NRC. On-site parking is not available.
- (b) Occasional travel to the NRC Regional locations and remote NRC facilities including State and Local Government facilities and external commercial and government application service providers and application hosting facilities, may be required. All travel, other than local travel, requires the prior approval of the Project Officer.
- (c) Total expenditure for domestic travel (does not include travel to NRC Headquarters) may not exceed the NOT TO EXCEED amounts listed in Section B of this contract, for each year of the period of performance, without the prior approval of the contracting officer. Please note: Profit/fee shall not be added to any travel performed. G&A is included in the travel (not to exceed) line items reflected in the contract. All G&A will be reimbursed in accordance with DCAA approved billing rates.
- (d) The contractor is encouraged to use Government contract airlines, AMTRAK rail services, and discount hotel/motel properties in order to reduce the cost of travel under this contract. The contracting officer shall, upon request, provide each traveler with a letter of identification which is required in order to participate in this program. The Federal Travel Directory (FTD) identifies carriers, contract fares, schedules, payment conditions, and hotel/motel properties which offer their services and rates to Government contractor personnel traveling on official business under this contract. The FTD, which is issued monthly, may be purchased from the U.S. Government Printing Office, Washington, DC 20402.
- (e) The contractor will be reimbursed for reasonable travel costs incurred directly and specifically in the performance of this contract. The cost limitations for travel costs are determined in accordance with the specific travel regulations cited in FAR 31.205-46, as are in effect on the date of the trip. Travel costs for research and related activities performed at State and nonprofit institutions, in accordance with section 12 of Public Law 100-679, shall be charged in accordance with the contractor's institutional policy to the degree that the limitations of Office of Management and Budget (OMB) guidance are not exceeded. Applicable guidance documents include OMB Circular A-87, Cost Principles for State and Local Governments; OMB Circular A-122, Cost principles for Nonprofit Organizations; and OMB Circular A-21, Cost Principles for Educational Institutions.
- (f) When the Government changes the Federal Travel Regulations, or other applicable regulations, it is the responsibility of the contractor to notify the contracting officer in accordance with the Limitations of Cost clause of the GSA contract if the contractor will be unable to make all of the approved trips and remain within the travel costs and limitations of this contract due to the changes.

5.0 PERSONNEL REQUIREMENTS

The Contractor shall maintain a pool of 2-3 pre-cleared staff including personnel with active security clearances in order to expedite the security clearance process. "Q" or equivalent Top Secret clearances are preferable. This pool of personnel shall be utilized to supplement the Contractor's proposed project team in order to ensure continuity of service as new task orders are issued or emergent security certification and FISMA compliance work is identified.

The Contractor shall have the professional communication skills required to take the necessary actions to contact, meet with, discuss, and otherwise obtain information required to accomplish the items described in this Statement of Work on his/her own initiative without supervision.

6.0 SPECIAL PERSONNEL REQUIREMENTS

The Contractor shall provide contact information (e.g. telephone numbers) of the Project Manager and designated alternate(s) in case these persons must be contacted outside of normal duty hours. These personnel will be expected to respond to all inquiries, both during and outside of normal duty hours, within one (1) hour.

7.0 GOVERNMENT-FURNISHED INFORMATION

The Government shall furnish available information (e.g. Standard Operational Procedures, regulations, manuals, texts, briefs and the other materials associated with this project), as well as access to the Rational Suite Enterprise Tools located and maintained on the NRC network infrastructure. All information, regardless of media, provided by the Government and/or generated for the Government in the performance of this contract are Government property and shall be maintained and disposed by the Government. At the time of disposition, the Contractor shall box, label contents, and deliver as directed by the Contracting Officer.

8.0 DELIVERABLES

- (a) The Contractor shall develop and deliver a Quality Assurance Plan for the program. This Plan must be accepted by the NRC prior to commencement of formal deliverable submissions. The Plan shall address the following:

Inspection System: A description of the inspection system to cover all efforts described in this Statement of Work. The description shall include specifics as to the areas to be inspected on both a scheduled or unscheduled basis, frequency of inspections, and the titles of the individuals who shall perform the inspection and their organizational placement.

Deficiency Prevention: A description of the methods to be used for identifying and preventing deficiencies and their causes in the quality of service performed before the level of performance becomes unacceptable.

Inspection Files: A description of the records to be maintained to document all inspections conducted by the Contractor and the necessary corrective or preventive actions taken. This document and the records of inspections completed shall be made readily available to the Government during the term of the contract.

- (b) 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. Specific requirements for these deliverables are as follows:

Integrated Security Activity Project Plan: The project plan shall 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 to accomplish the work, identify the resources needed to complete the work, and allocate the effort required in the specified time frame for the completion of each of the tasks in the WBS shall be included. 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.

Microsoft Project Plan that incorporates 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.

Integrated Security Activity Scheduling: Contractor staff shall develop and maintain an integrated security schedule with resource utilization in MS-Project for all NRC security related activities, services, and deliverables.

- (c) The Contractor shall develop the following information security artifacts in support of NRC information systems certification and accreditation:

Certification Requirements	Major Application	General Support System	Listed System	E-Gov	Other
E-Authentication Risk Assessment	X	X	X	X	X
Security Categorization	X	X	X	X	X
Security Risk Assessment	X	X	X		
System Security Plan (Rational Suite Enterprise Deliverable)	X	X	X		
Security Test and Evaluation Plan (Test Procedures) (Rational Suite Enterprise Deliverable)	X	X			
Contingency Test Plan (Business Continuity (Test Procedures) (Rational Suite Enterprise Deliverable)	X	X			
Security Test and Evaluation Report (Rational Suite Enterprise Deliverable)	X	X			
Contingency Test Report (Rational Suite Enterprise Deliverable)	X	X			
Plan of Action and Milestones (Corrective Action Plan) (Rational Suite Enterprise Deliverable)	X	X			
Annual Analysis of Systems Documentation, Security Controls, Requirements, and Implementation Status Report	X	X			

Table 1

- (d) The Contractor may be required to develop the following information security services in support of NRC information systems certification and accreditation:

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

Review, Verification, and Validation of Security Controls and Requirements: The Contractor shall review, verify, and validate all security controls and security requirements and associated technical resolutions, risk mitigation, and implementations contained within various NRC security and systems development documentation or the Rational Suite Enterprise such that confirmation that the system and associated controls are operating as intended.

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

Development, Update and Maintenance of Common Control Sets and Procedures: The Contractor shall develop a standardized set of streamlined security certification and accreditation documentation that focuses on the functional alignment of common security control sets and standard operating procedures for LOW, MODERATE, and HIGH Baseline systems consistent with FISMA, and NIST SP 800-53 that integrate with the NRC PMM and EA within the Rational Suite Enterprise.

Security Engineering and Common Security Controls Support: The Contractor shall provide Security Engineering support for application development and information systems solution assessment and proposal such that information systems architectures proposed for implementation at the NRC are based on sound security engineering principles and practices. The contract shall support the NRC enterprise architecture staff in the development of the security line of business program and documentation, and support the NRC in the assessment, documentation, and implementation of common security solutions and OMB information systems security line of business integration.

Security Support for HSPD-12 Solution Definition, Analysis, Documentation, Development, Integration, and Deployment: The Contractor shall provide technical staff capable of documenting, integrating, implementing and supporting a certified and accredited HSPD-12 solution.

Security Support for IPV6 Solution Definition, Analysis, Documentation, Development, Integration, and Deployment: The Contractor shall provide technical staff capable of documenting, integrating, implementing and supporting a certified and accredited IPV6 solution.

Security Reporting: In addition to the applicable requirements, the Contractor shall provide a Plan of Action and Milestone Status Tracking Report, FISMA Compliance and Health Report, Risk and Security Vulnerability Trending Report, Security Scoping and Categorization Report, and Security Costs Report.

Security Regulations Analysis and Research: The Contractor shall monitor, research, and develop documentation and reports on government and private sector security and enterprise architecture related activities as to provide pro-active guidance to the NRC on possible future security related laws, regulations, guidance, and OMB Exhibit 300 and 53 support that may impact the integrated NRC security program. The Contractor shall support the NRC in the development of security and enterprise architecture related documentation as to ensure seamless integration of the two programs with a focus on migration of day-to-day NRC infrastructure and application systems to a modernized target state consistent with the latest OMB guidance and the Federal Enterprise Architecture.

Security Technology Integration and Implementation Solutions: The Contractor shall provide technical staff capable of implementing technical security solutions and risk mitigation strategies resulting from work identified under this contract on an as needed basis.

Annual Analysis of Systems Documentation, Security Controls, Requirements, and Implementation Status: The Contractor shall conduct on all "Major Applications" and "GSS" NRC systems an inclusive independent audit annually that shall include but is not limited to the review, verification, and validation of all current systems documentation, analysis, penetration, vulnerability, configuration, systems integrity, and patch management scans. The Contractor shall identify, analyze, and propose tested corrective actions that ensure the currency of the systems security posture and ensures that controls are operating as intended.

The Contractor shall identify NRC information systems security vulnerability trends at an agency and system level with special attention to those deficiencies that would impact NRC FISMA compliance.

Security Tools Support: The Contractor shall provide technical support services to develop, implement, administer, and maintain the information systems tools that support the NRC's ISS program including: Rational ClearCase, ClearQuest, RequisitePro, TestManager, MethodeComposer, XML, Microsoft Office 2003 (Word, Excel, Access, PowerPoint, Visio, InfoPath, Project Professional) XML Integration, Crystal Reports, Crystal Enterprise Server, and Microsoft SharePoint Portal. The Contractor shall also develop procedures for the use, administration, and maintenance of these tools and associated security deliverables produced, stored and supported by these tools. The Contractor shall support the NRC by providing data entry and web page development services to ensure the integrity and currency of the information stored in the tools supporting the ISS program. The Contractor shall also provide testing support, using a structured testing methodology approved by the NRC.

Security Program Communications Support: The Contractor shall support the NRC in communicating the ISS program's processes and on the use of the associated information systems tools. The Contractor shall utilize the Rational Method Composer to develop Intranet, web based process flows and procedures.

8.1 Deliverable Standards

All deliverables shall be delivered no later than the date specified in the task order. Deliverables are to be transmitted with a cover letter, on the prime Contractor's letterhead, describing the contents and identifying task order number and title.

8.1.1 Performance Measures

8.1.1.1 Description: 100 % compliance with Sections 8.1.2 through 8.1.10 and 9.0. The Contractor shall monitor, evaluate, and trend a random sampling of draft and final deliverables for adherence to requirements. The results of the evaluations, trend analysis, and institutional correction actions will be collected and reported in the Monthly Progress Report. The purpose of the evaluations is to help confirm that the information provided meets or exceeds the quality performance metric and that quality issues are identified and corrected before they impact contractor performance. Compliance will be monitored via Project Officer final deliverable submission acceptance.

- i. Target: Quality performance metric = 100%**
- ii. Data Source: Final Deliverables and Monthly Progress Reports**
- iii. Responsible Party: Contractor**
- iv. Frequency: Monthly**

8.1.1.2 Description: 100 % compliance with Sections 8.1.2 through 8.1.10 and 9.0. Compliance will be monitored via Project Officer final deliverable submission acceptance. The Project Officer shall monitor and evaluate a random sampling of deliverables in contrast to contract evaluations and trend analyzes. The results of the evaluations will be collected and reported to the Contractor in order to ensure continued improvement in product quality. The purpose of the evaluations is to help ensure alignment between NRC and Contractor quality expectations and confirm that the information provided meets or exceeds the quality performance metric. Compliance will be monitored via Project Officer final deliverable submission acceptance.

- i. Target: Quality performance metric = 100%**
- ii. Data Source: Final Deliverables and Monthly Progress Reports**
- iii. Responsible Party: Contractor**
- iv. Frequency: Monthly**

8.1.1.3 Description: The Contractor develop deliverables as specified in ENCLOSURE 6 - C&A PROCESS AND DELIVERABLES that comply with NIST and FISMA guidance, and NRC PMM Security Document Templates (Provided at time of contract award) such that approval of final deliverables by NRC SITSO/DAA may be achieved within one (1) iterative cycle and no more than three (3) business day deliverable schedule slippage. The Contractor shall monitor and evaluate a random sampling of deliverables. The results of the evaluations will be collected and reported in the Monthly Progress Report. The purpose of the evaluations is to help confirm that the information provided meets or exceeds the quality performance metric. Compliance will be monitored via Project Officer final deliverable submission acceptance. The Contractor shall comply

with all National Information Assurance Certification and Accreditation Process (NIACAP) and National Security Agency (NSA) guidance for the certification and accreditation of NRC classified systems.

- i. **Target: Quality performance metric $\geq 95\%$**
- ii. **Data Source: Final Deliverables, Project Schedule, Monthly Progress Reports, NIST and FISMA Guidance and PMM Security Document Templates**
- iii. **Responsible Party: Contractor**
- iv. **Frequency: Monthly**

8.1.1.4 Description: 100% of deliverables milestones shall be delivered to the Project Officer within the mutually agreed project schedule. Change in final deliverable milestones in the project schedule shall be mutually acceptable and shall be approved by the Project Officer. Compliance will be monitored via Project Officer through Project Schedule and Monthly Progress Reports reviews.

- i. **Target: 100% by agreed date**
- ii. **Data Source: Project Schedule and Monthly Progress Reports**
- iii. **Responsible Party: Contractor**
- iv. **Frequency: Quarterly**

8.1.1.5 Description: 100% of final project deliverables, overall project estimates, and actual costs shall be on target with mutually agreed project schedule and accepted task order proposal costs. Compliance will be monitored via Project Officer through Project Schedule and Monthly Progress Reports reviews.

- i. **Target: 100% by agreed date**
- ii. **Data Source: Project Schedule and Monthly Progress Reports**
- iii. **Responsible Party: Contractor**
- iv. **Frequency: Quarterly**

8.1.1.6 Description: Level of customer satisfaction as measured by the NRC Customer Satisfaction Survey. Customer Satisfaction Surveys from the NRC staff, Contracting Officer, or Project Officer periodic site visits, and/or customer complaints will also be compiled by the Project Officer and reviewed in order to determine the Contractor's performance level.

- i. **Target: 90%**
- ii. **Data Source: NRC Customer Survey**
- iii. **Responsible Party: NRC**
- iv. **Frequency: Quarterly**

8.1.1.7 Description: The number of business days required to take corrective action on issues identified in a Contract Discrepancy Report (CDR), as referenced in Section 8.1.7. Compliance will be monitored via the Project Officer through Draft Deliverables, Final Deliverables, Project Schedule, Monthly Progress Reports, NIST and FISMA Guidance, PMM Security Document Templates, and Project Officer review of related NRC Customer Satisfaction Surveys.

- i. **Target: three (3) business days of the CDR Issuance meeting**
- ii. **Data Source: Draft Deliverables, Final Deliverables, Project Schedule, Monthly Progress Reports, NIST and FISMA Guidance, PMM Security Document Templates, and Project Officer review of related NRC Customer Satisfaction Surveys.**
- iii. **Responsible Party: Contractor**
- iv. **Frequency: As needed upon issuance of a CDR**
- v. **Process & Exceptions: The duration will be determined from the time of CDR Issuance meeting. The 3 business day corrective action time will not include time in which the Contractor is waiting on the NRC for data necessary to perform the corrective action.**

8.1.2 Deliverable File Formats

The Contractor shall provide all documentation to the NRC Project Officer electronically via e-mail in all the following formats, except as specifically stated herein: Microsoft Word (version 2003), Microsoft Excel (version 2003), Microsoft Project (version 2003), and Adobe PDF (version 7.0) formats.

8.1.3 Standard for Grammar and Mechanics

All documentation submitted by the Contractor shall conform to the *Chicago Manual of Style*, as amended by any applicable NRC format templates and requirements.

8.1.4 Timeliness and Accuracy

Timeliness and accuracy are indicators of standard of performance.

8.1.5 Draft and Final Submission

All documentation shall be submitted in draft form for comment by the Government and reviewed in order to determine the Contractor's performance level.

8.1.6 Draft and Final Submission

All documentation shall be submitted in draft form for comment to the NRC Project Officer.

The Contractor shall incorporate into the final deliverable documentation any NRC comments received on the draft documentation within 3 business days of receipt of comments from the NRC Project Officer.

The NRC Project Officer will review all draft documents submitted as part of contract deliverables for conformity to the standards referenced in this Statement of Work. Any changes required after the first revision cycle shall be completed at no additional cost to the Government. The first revision cycle for a deliverable shall be acceptable to the Government when the Contractor submits a revised deliverable incorporating any comments and suggestions made by the NRC Project Officer on his review of the initial draft.

The following provisions also apply to all deliverables:

Reporting Requirements: In addition to meeting the delivery schedule in the timely submission of any draft and final reports, summaries, data and documents that are created in the performance of this contract, the Contractor shall comply with the directions of the NRC regarding the contents of the report, summaries, data and related documents to include correcting, deleting, editing, revising, modify, formatting, and supplementing any of the information contained therein at no additional cost to the NRC. Performance under the contract will not be deemed accepted or completed until the NRC's directions are complied with. The reports, summaries, data and related documents will be considered draft until approved by the NRC. The Contractor agrees that the direction, determinations, and decisions on approval or disapproval of reports, summaries, data and related documents created under this contract remains solely within the discretion of the NRC.

Publication of Results: Prior to any dissemination, display, publication or release of articles, reports, summaries, data or related documents developed under the contract, the Contractor shall submit for review and approval by the NRC the proposed articles, reports, summaries, data and related documents that the Contractor intends to release, disseminate or publish to other persons, the public or any other entities. The Contractor shall not release, disseminate, display or publish articles, reports, summaries, data, and related documents or the contents therein that have not been reviewed and approved by the NRC for release, display, dissemination or publication. The Contractor agrees to conspicuously place any disclaimers, markings or notices directed by the NRC on any articles, reports, summaries, data and related documents that the Contractor intends to release, display, disseminate or publish to other persons, the public or any other entities. The Contractor agrees and grants a royalty free, nonexclusive, irrevocable world-wide license to the government to use, reproduce, modify, distribute, prepare derivative works, release, display or disclose the articles, reports, summaries, data and related documents developed under the contract, for any governmental purpose and to have or authorize others to do so.

Identification/ Marking of Sensitive and Safeguards Information: The decision, determination or direction by the NRC that information constitutes sensitive or safeguards information remains exclusively a matter within the authority of the NRC to make. In performing the contract, the Contractor shall clearly mark sensitive unclassified non-safeguards information (SUNSI), sensitive, and safeguards information to include for example Official Use Only and Safeguards Information on any reports, documents, designs, data, materials and written information as directed by the NRC. In addition to marking the information as directed by the NRC, the Contractor shall use the applicable NRC cover sheet forms (e.g. NRC Form 461 Safeguards Information and NRC Form 190B Official Use Only) in maintaining these records and documents. The Contractor will ensure that sensitive and safeguards information is handled appropriately, maintained and protected from unauthorized disclosure. The Contractor shall comply with the requirements to mark, maintain and protect all information including documents, summaries, reports, data, designs, and materials in accordance with the provisions of Section 147 of the Atomic Energy Act of 1954 as amended, its implementing regulations (10 CFR 73.21), and NRC Management Directive and Handbook 12.6.

Remedies: In addition to any civil, criminal and contractual remedies available under the applicable laws and regulations, failure to comply with the above provisions and or NRC directions may result in suspension, withholding or offsetting of any payments invoiced or claimed by the Contractor. If the Contractor intends to enter into any subcontracts or other agreements to perform this contract, the Contractor shall include all the above provisions in any subcontract or agreements.

Additional written reports may be required and negotiated.

8.1.7 Deliverable Reviews

Deliverable Reviews will be held to provide the Contractor with feedback related to improving the quality of deliverables, including feedback received from Customer Satisfaction Surveys. Such reviews will be coordinated by the NRC Project Officer as required to supplement written comments provided on deliverable submissions. The written minutes of all deliverable review meetings shall be prepared by the Government. Should the Contractor not concur with the minutes, the Contractor shall so state any areas of non-concurrence in writing to the Project Officer within ten calendar days of receipt of the minutes. Failure to correct and identify defects, and integrate the Project Officer's comments into the deliverable may result in the issuance of a Contract Discrepancy Report (CDR). Upon issuance of a CDR, a meeting will be held.

8.1.8 Monthly Progress Reports

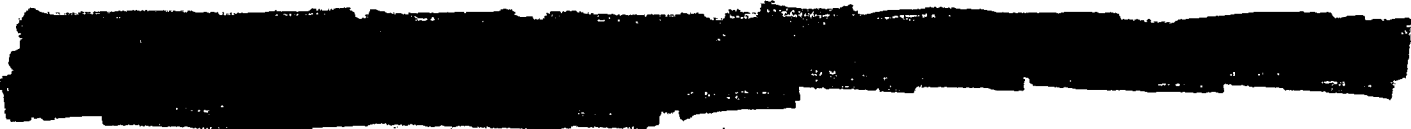
Monthly Progress Reports must be submitted to the Project Officer no later than the 5th workday of every month. Progress reports must be submitted on the prime Contractor's letterhead and be accompanied by a copy of that month's invoice, with written approval of the invoice by the Project Officer. Progress reports must contain the information in ENCLOSURE 2 – MONTHLY PROGRESS REPORT FORMAT.

8.1.9 Daily Quick-Look Status Reports

The Daily Quick-Look Status Reports shall be submitted to the Project Officer no later than the 7:00 AM Eastern Standard Time each work day. The Daily Quick-Look Status Report shall contain; a graphical deliverable indicator chart illustrating completion status, a detailed deliverable table by system with each deliverable and key deliverable milestones listed, associated resources and estimated and actual completion dates, and challenges to completion of the deliverable within schedule.

8.1.10 Other Reporting Requirements

The Contractor shall bring problems or potential problems affecting performance to the attention of the Project Officer and Contracting Officer as soon as possible. Verbal reports will be followed up with written reports when directed by the Project Officer.



9.0 SPECIFIC TASKS

The Contractor shall provide security analyst staff and develop all requisite systems certification and accreditation documentation such that all systems obtain an Authorization to Operate (ATO).

The Contractor shall provide a security analyst staff and the development of the associated documentation associated with the deliverables identified in SECTION 8.0 DELIVERABLES, and security support tasks specified in ENCLOSURE 6 – C&A PROCESS AND DELIVERABLES of this SOW for LOW, MODERATE, and HIGH Baseline systems for each system category Major Applications, General Support System, E-Government (E-Gov), Listed, and Other.

9.1 NRC Security Certification and Accreditation Processes

For those NRC software applications that have been determined by the OIS and the sponsor to be systems, the Contractor shall utilize either the NRC Unclassified or Classified security certification and accreditation process:

9.2 ISS Program Unclassified

The Contractor shall utilize the Rational Suite Enterprise in the certification and accreditation of NRC information systems. This will enable leveraging of common security controls and solutions stored and automatically populated for an individual project within the Rational Suite Enterprise. A summary of the certification and accreditation process for unclassified information systems is provided below in Chart 1:

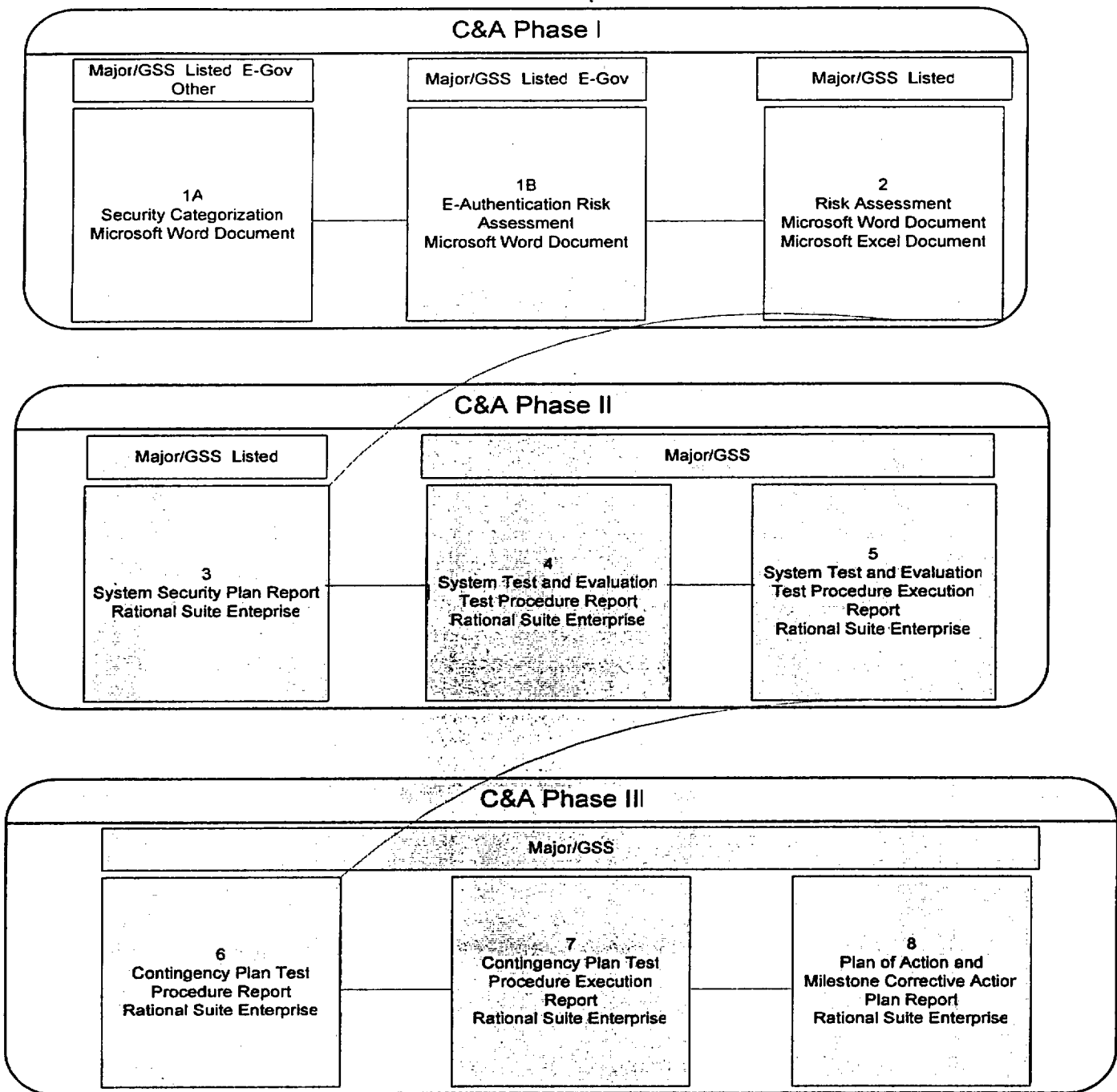


CHART 1

9.3 ISS Program Classified

The Contractor shall support the NRC staff in the development of hard copy certification and accreditation documentation consistent with NIACAP for Designated Accreditation Authority (DAA) review and approval of classified NRC information systems. The Contractor shall comply with all NIACAP and National Security Agency (NSA) guidance for the certification and accreditation of NRC classified systems. All documentation shall be consistent with compartmented and trusted information systems security engineering principles and shall comply with National Security Systems and Intelligence Systems classified/trusted information systems application development, and security certification and accreditation guidance. The Contractor shall deliver all NIACAP documentation in electronic format (CD, Microsoft Word 2003).

All classified information provided or generated pursuant to this contract shall be protected as follows:

- The Contractor shall not disclose the classified information to a third party government, person, or firm, or representative thereof, without the prior written consent of the releasing government.
- The Contractor shall provide the classified information a degree of protection no less stringent than that provided by the releasing government in accordance with National Security regulations and as prescribed by its National Security Authority/Designated Security Authority (NSA/DSA).
- The Contractor shall not use the classified information for any purpose other than for which it was provided or generated, without the prior written consent of the releasing government.
- All classified information provided or generated pursuant to this contract shall be transferred internationally only through government channels or as specified in writing by the Governments concerned.
- All classified information shall only be disclosed to individuals who have an official need-to-know for the performance of the contract and who have a Personnel Security Clearance at least equal to the classification of the information involved.
- All classified information provided pursuant to this contract shall be marked by the recipient with its government's equivalent security classification.
- All classified information generated pursuant to this contract shall be assigned a security classification in accordance with the security classification specifications.
- All cases in which it is known or there is reason to suspect, that classified information provided or generated pursuant to this contract has been lost or disclosed to unauthorized persons, shall be reported promptly and fully in accordance with National Regulations.
- All classified materials no longer required shall be destroyed or returned to the originator.
- All classified information provided or generated pursuant to this contract shall not be further provided to another potential Contractor or subcontractor unless:
 - Written assurance is obtained from the recipients NSA/DSA to the effect that the potential Contractor or subcontractor has been approved for access to CLASSIFIED information by its NSA/DSA; and
 - Written consent is obtained from the contracting authority for the prime contract if the potential subcontractor is located in a country outside the continental United States.

All classified information and material provided or generated under this contract will continue to be protected in the event of withdrawal by the recipient party or upon termination of the contract, in accordance with national regulations.

10.0 POST AWARD MEETING

The Government will schedule a kick-off meeting within five (5) business days after contract award or upon security clearance authorization. The Project Officer will provide an agenda prior to the meeting. The Contractor shall participate in the meeting to establish process, procedures and priority of tasking. The Contracting Officer, the Project Officer, and the Project Officer's technical personnel will represent the Government. The Contractor shall have equivalent representation at the meeting.

Following the kick-off meeting, the Contractor shall meet at least weekly with the Project Officer during the first month of the contract. Subsequent meetings will be scheduled on a regular basis.

SOW Enclosures:

ENCLOSURE 1 - NRC FORM 187 - CONTRACT SECURITY AND/OR CLASSIFICATION REQUIREMENTS

ENCLOSURE 2 - MONTHLY PROGRESS REPORT FORMAT

ENCLOSURE 3 - RESERVED

ENCLOSURE 4 - REFERENCES

ENCLOSURE 5 - TERMS AND DEFINITIONS

ENCLOSURE 6 - C&A PROCESS AND DELIVERABLES



D. ORDER TERMS, CONDITIONS, AND REQUIREMENTS

D.1 CLAUSES INCORPORATED BY REFERENCE

This contract will incorporate one or more clauses by reference, with the same force and effect as if they were given in full text, if they are not already included in the Offeror's GSA Schedule contract. Upon request, the Contracting Officer will make their full text available. Also, the full text of a clause may be accessed electronically at this address: <http://www.arnet.gov/far>

NUMBER	TITLE	DATE
52.232-1	PAYMENTS	APR 1984
52.232-7	PAYMENTS UNDER TIME-AND-MATERIALS AND LABOR-HOUR CONTRACTS	AUG 2005
52.232-18	AVAILABILITY OF FUNDS	APR 1984
52.232-22	LIMITATION OF FUNDS	APR 1984
52.227-14	RIGHTS IN DATA--GENERAL	JUN 1987
52.224-1	PRIVACY ACT NOTIFICATION	APR 1984
52.224-2	PRIVACY ACT	APR 1984
52.243-3	CHANGES -- TIME-AND-MATERIALS OR LABOR-HOURS	SEPT 2000

D.2 CLAUSES INCORPORATED IN FULL TEXT

FAR 52.217-9, Option to Extend the Term of the Contract (MAR 2000)

- (a) The Government may extend the term of this delivery order by written notice to the delivery order or within 60 days of the expiration date of the delivery order; provided that the Government gives the delivery order or a preliminary written notice of its intent to extend at least 15 days before the delivery order expires. The preliminary notice does not commit the Government to an extension.
- (b) If the Government exercises this option, the extended delivery order shall be considered to include this option clause.
- (c) The total duration for this delivery order, including the exercise of any options under this clause, shall not exceed July 30, 2011.

FAR 52.232-19, Availability of Funds for the Next Fiscal Year (APR 1984)

Funds are not presently available for performance under this contract beyond July 30, 2007. The Government's obligation for performance of this contract beyond that date is contingent upon the availability of appropriated funds from which payment for contract purposes can be made. No legal liability on the part of the Government for any payment may arise for performance under this contract beyond July 30, 2007, until funds are made available to the Contracting Officer for performance and until the Contractor receives notice of availability, to be confirmed in writing by the Contracting Officer.

FAR 52.244-2, Subcontracts (AUG 1998)

(a) *Definitions.* As used in this clause—

"Approved purchasing system" means a Contractor's purchasing system that has been reviewed and approved in accordance with Part 44 of the Federal Acquisition Regulation (FAR).

"Consent to subcontract" means the Contracting Officer's written consent for the Contractor to enter into a particular subcontract.

"Subcontract" means any contract, as defined in FAR Subpart 2.1, entered into by a subcontractor to furnish supplies or services for performance of the prime contract or a subcontract. It includes, but is not limited to, purchase orders, and changes and modifications to purchase orders.

(b) This clause does not apply to subcontracts for special test equipment when the contract contains the clause at FAR 52.245-18, Special Test Equipment.

(c) When this clause is included in a fixed-price type contract, consent to subcontract is required only on unpriced contract actions (including unpriced modifications or unpriced delivery orders), and only if required in accordance with paragraph (d) or (e) of this clause.

(d) If the Contractor does not have an approved purchasing system, consent to subcontract is required for any subcontract that—

- (1) Is of the cost-reimbursement, time-and-materials, or labor-hour type; or
- (2) Is fixed-price and exceeds—

(i) For a contract awarded by the Department of Defense, the Coast Guard, or the National Aeronautics and Space Administration, the greater of the simplified acquisition threshold or 5 percent of the total estimated cost of the contract; or

(ii) For a contract awarded by a civilian agency other than the Coast Guard and the National Aeronautics and Space Administration, either the simplified acquisition threshold or 5 percent of the total estimated cost of the contract.

(e) If the Contractor has an approved purchasing system, the Contractor nevertheless shall obtain the Contracting Officer's written consent before placing the following subcontracts:

(f)(1) The Contractor shall notify the Contracting Officer reasonably in advance of placing any subcontract or modification thereof for which consent is required under paragraph (c), (d), or (e) of this clause, including the following information:

(i) A description of the supplies or services to be subcontracted.

(ii) Identification of the type of subcontract to be used.

(iii) Identification of the proposed subcontractor.

(iv) The proposed subcontract price.

(v) The subcontractor's current, complete, and accurate cost or pricing data and Certificate of Current Cost or Pricing Data, if required by other contract provisions.

(vi) The subcontractor's Disclosure Statement or Certificate relating to Cost Accounting Standards when such data are required by other provisions of this contract.

(vii) A negotiation memorandum reflecting—

(A) The principal elements of the subcontract price negotiations;

(B) The most significant considerations controlling establishment of initial or revised prices;

(C) The reason cost or pricing data were or were not required;

(D) The extent, if any, to which the Contractor did not rely on the subcontractor's cost or pricing data in determining the price objective and in negotiating the final price;

(E) The extent to which it was recognized in the negotiation that the subcontractor's cost or pricing data were not accurate, complete, or current; the action taken by the Contractor and the subcontractor; and the effect of any such defective data on the total price negotiated;

(F) The reasons for any significant difference between the Contractor's price objective and the price negotiated; and

(G) A complete explanation of the incentive fee or profit plan when incentives are used. The explanation shall identify each critical performance element, management decisions used to quantify each incentive element, reasons for the incentives, and a summary of all trade-off possibilities considered.

(2) The Contractor is not required to notify the Contracting Officer in advance of entering into any subcontract for which consent is not required under paragraph (c), (d), or (e) of this clause.

(g) Unless the consent or approval specifically provides otherwise, neither consent by the Contracting Officer to any subcontract nor approval of the Contractor's purchasing system shall constitute a determination—

(1) Of the acceptability of any subcontract terms or conditions;

(2) Of the allowability of any cost under this contract; or

(3) To relieve the Contractor of any responsibility for performing this contract.

(h) No subcontract or modification thereof placed under this contract shall provide for payment on a cost-plus-a-percentage-of-cost basis, and any fee payable under cost-reimbursement type subcontracts shall not exceed the fee limitations in FAR 15.404-4(c)(4)(i).

(i) The Contractor shall give the Contracting Officer immediate written notice of any action or suit filed and prompt notice of any claim made against the Contractor by any subcontractor or vendor that, in the opinion of the Contractor, may result in litigation related in any way to this contract, with respect to which the Contractor may be entitled to reimbursement from the Government.

(j) The Government reserves the right to review the Contractor's purchasing system as set forth in FAR Subpart 44.3.

(k) Paragraphs (d) and (f) of this clause do not apply to the following subcontracts, which were evaluated during negotiations:

D.3 SECURITY (MAR 2004)

(a) Contract Security and/or Classification Requirements (NRC Form 187). The policies, procedures, and criteria of the NRC Security Program, NRC Management Directive (MD) 12 (including MD 12.1, "NRC Facility Security

Program;" MD 12.2, "NRC Classified Information Security Program;" MD 12.3, "NRC Personnel Security Program;" MD 12.4, "NRC Telecommunications Systems Security Program;" MD 12.5, "NRC Automated Information Systems Security Program;" and MD 12.6, "NRC Sensitive Unclassified Information Security Program"), apply to performance of this contract, subcontract or other activity. This MD is incorporated into this contract by reference as though fully set forth herein. The attached NRC Form 187 (See List of Attachments) furnishes the basis for providing security and classification requirements to prime contractors, subcontractors, or others (e.g., bidders) who have or may have an NRC contractual relationship that requires access to classified Restricted Data or National Security Information or matter, access to sensitive unclassified information (e.g., Safeguards), access to sensitive Information Technology (IT) systems or data, unescorted access to NRC controlled buildings/space, or unescorted access to protected and vital areas of nuclear power plants.

(b) It is the contractor's duty to protect National Security Information, Restricted Data, and Formerly Restricted Data. The contractor shall, in accordance with the Commission's security regulations and requirements, be responsible for protecting National Security Information, Restricted Data, and Formerly Restricted Data, and for protecting against sabotage, espionage, loss, and theft, the classified documents and material in the contractor's possession in connection with the performance of work under this contract. Except as otherwise expressly provided in this contract, the contractor shall, upon completion or termination of this contract, transmit to the Commission any classified matter in the possession of the contractor or any person under the contractor's control in connection with performance of this contract. If retention by the contractor of any classified matter is required after the completion or termination of the contract and the retention is approved by the contracting officer, the contractor shall complete a certificate of possession to be furnished to the Commission specifying the classified matter to be retained. The certification must identify the items and types or categories of matter retained, the conditions governing the retention of the matter and their period of retention, if known. If the retention is approved by the contracting officer, the security provisions of the contract continue to be applicable to the matter retained.

(c) In connection with the performance of the work under this contract, the contractor may be furnished, or may develop or acquire, safeguards information, or confidential or privileged technical, business, or financial information, including Commission plans, policies, reports, financial plans, internal data protected by the Privacy Act of 1974 (Pub. L. 93.579), or other information which has not been released to the public or has been determined by the Commission to be otherwise exempt from disclosure to the public. The contractor shall ensure that information protected from public disclosure is maintained as required by NRC regulations and policies, as cited in this contract or as otherwise provided by the NRC. The contractor will not directly or indirectly duplicate, disseminate, or disclose the information in whole or in part to any other person or organization except as may be necessary to perform the work under this contract. The contractor agrees to return the information to the Commission or otherwise dispose of it at the direction of the contracting officer. Failure to comply with this clause is grounds for termination of this contract.

(d) Regulations. The contractor agrees to conform to all security regulations and requirements of the Commission which are subject to change as directed by the NRC Division of Facilities and Security (DFS) and the Contracting Officer. These changes will be under the authority of the FAR Changes clause referenced in this document.

The contractor agrees to comply with the security requirements set forth in NRC Management Directive 12.1, NRC Facility Security Program which is incorporated into this contract by reference as though fully set forth herein. Attention is directed specifically to the section titled "Infractions and Violations," including "Administrative Actions" and "Reporting Infractions."

(e) Definition of National Security Information. The term National Security Information, as used in this clause, means information that has been determined pursuant to Executive Order 12958 or any predecessor order to require protection against unauthorized disclosure and that is so designated.

(f) Definition of Restricted Data. The term Restricted Data, as used in this clause, means all data concerning design, manufacture, or utilization of atomic weapons; the production of special nuclear material; or the use of special nuclear material in the production of energy, but does not include data declassified or removed from the Restricted Data category pursuant to Section 142 of the Atomic Energy Act of 1954, as amended.

(g) Definition of Formerly Restricted Data. The term Formerly Restricted Data, as used in this clause, means all data removed from the Restricted Data category under Section 142-d of the Atomic Energy Act of 1954, as amended.

(h) **Definition of Safeguards Information.** Sensitive unclassified information that specifically identifies the detailed security measures of a licensee or an applicant for the physical protection of special nuclear material; or security measures for the physical protection and location of certain plant equipment vital to the safety of production of utilization facilities. Protection of this information is required pursuant to Section 147 of the Atomic Energy Act of 1954, as amended.

(i) **Security Clearance.** The contractor may not permit any individual to have access to Restricted Data, Formerly Restricted Data, or other classified information, except in accordance with the Atomic Energy Act of 1954, as amended, and the Commission's regulations or requirements applicable to the particular type or category of classified information to which access is required. The contractor shall also execute a Standard Form 312, Classified Information Nondisclosure Agreement, when access to classified information is required.

(j) **Criminal Liabilities.** It is understood that disclosure of National Security Information, Restricted Data, and Formerly Restricted Data relating to the work or services ordered hereunder to any person not entitled to receive it, or failure to safeguard any Restricted Data, Formerly Restricted Data, or any other classified matter that may come to the contractor or any person under the contractor's control in connection with work under this contract, may subject the contractor, its agents, employees, or subcontractors to criminal liability under the laws of the United States. (See the Atomic Energy Act of 1954, as amended, 42 U.S.C. 2011 et seq.; 18 U.S.C. 793 and 794; and Executive Order 12958.)

(k) **Subcontracts and Purchase Orders.** Except as otherwise authorized in writing by the contracting officer, the contractor shall insert provisions similar to the foregoing in all subcontracts and purchase orders under this contract.

(l) In performing the contract work, the contractor shall classify all documents, material, and equipment originated or generated by the contractor in accordance with guidance issued by the Commission. Every subcontract and purchase order issued hereunder involving the origination or generation of classified documents, material, and equipment must provide that the subcontractor or supplier assign classification to all documents, material, and equipment in accordance with guidance furnished by the contractor.

D.4 SECURITY REQUIREMENTS FOR INFORMATION TECHNOLOGY ACCESS APPROVAL (FEB 2004)

The proposer/contractor must identify all individuals and propose the level of Information Technology (IT) approval for each, using the following guidance. The NRC sponsoring office shall make the final determination of the level, if any, of IT approval required for all individuals working under this contract.

The Government shall have and exercise full and complete control over granting, denying, withholding, or terminating building access approvals for individuals performing work under this contract.

SECURITY REQUIREMENTS FOR LEVEL I

Performance under this contract will involve prime contractor personnel, subcontractors or others who perform services requiring direct access to or operate agency sensitive information technology systems or data (IT Level I).

The IT Level I involves responsibility for the planning, direction, and implementation of a computer security program; major responsibility for the direction, planning, and design of a computer system, including hardware and software; or the capability to access a computer system during its operation or maintenance in such a way that could cause or that has a relatively high risk of causing grave damage; or the capability to realize a significant personal gain from computer access. Such contractor personnel shall be subject to the NRC contractor personnel security requirements of NRC Management Directive (MD) 12.3, Part I and will require a favorably adjudicated Limited Background Investigation (LBI).

A contractor employee shall not have access to sensitive information technology systems or data until he/she is approved by Security Branch, Division of Facilities and Security (SB/DFS). Temporary access may be approved based on a favorable adjudication of their security forms and checks. Final access will be approved based on a favorably adjudicated LBI in accordance with the procedures found in NRC MD 12.3, Part I. However, temporary access authorization approval will be revoked and the employee may subsequently be removed from the contract in the event the employee's investigation cannot be favorably adjudicated. Such employee will not be authorized to

work under any NRC contract without the approval of SB/DFS. Timely receipt of properly completed security applications is a contract requirement. Failure of the contractor to comply with this condition within the ten work-day period may be a basis to void the notice of selection. In that event, the Government may select another firm for award. When an individual receives final access, the individual will be subject to a reinvestigation every 10 years.

The contractor shall submit a completed security forms packet, including the SF-86, "Questionnaire for National Security Positions," and fingerprint charts, through the Project Officer to SB/ DFS for review and favorable adjudication, prior to the individual performing work under this contract. The contractor shall assure that all forms are accurate, complete, and legible (except for Part 2 of the questionnaire, which is required to be completed in private and submitted by the individual to the contractor in a sealed envelope), as set forth in MD 12.3 which is incorporated into this contract by reference as though fully set forth herein. Based on SB review of the applicant's security forms and/or the receipt of adverse information by NRC, the individual may be denied access to NRC facilities, sensitive information technology systems or data until a final determination is made of his/her eligibility under the provisions of MD 12.3. Any questions regarding the individual's eligibility for IT Level I approval will be resolved in accordance with the due process procedures set forth in MD 12.3 and E. O. 12968.

In accordance with NRCAR 2052.204.70 "Security," IT Level I contractors shall be subject to the attached NRC Form 187 (See Section J for List of Attachments) which furnishes the basis for providing security requirements to prime contractors, subcontractors or others (e.g., bidders) who have or may have an NRC contractual relationship which requires access to or operation of agency sensitive information technology systems or remote development and/or analysis of sensitive information technology systems or data or other access to such systems and data; access on a continuing basis (in excess of 30 days) to NRC Headquarters controlled buildings; or otherwise requires issuance of an NRC badge.

SECURITY REQUIREMENTS FOR LEVEL II

Performance under this contract will involve contractor personnel that develop and/or analyze sensitive information technology systems or data or otherwise have access to such systems or data (IT Level II).

The IT Level II involves responsibility for the planning, design, operation, or maintenance of a computer system and all other computer or IT positions. Such contractor personnel shall be subject to the NRC contractor personnel requirements of MD 12.3, Part I, which is hereby incorporated by reference and made a part of this contract as though fully set forth herein, and will require a favorably adjudicated Access National Agency Check with Inquiries (ANACI).

A contractor employee shall not have access to sensitive information technology systems or data until he/she is approved by SB/DFS. Temporary access may be approved based on a favorable review of their security forms and checks. Final access will be approved based on a favorably adjudicated ANACI in accordance with the procedures found in MD 12.3, Part I. However, temporary access authorization approval will be revoked and the employee may subsequently be removed from the contract in the event the employee's investigation cannot be favorably adjudicated. Such employee will not be authorized to work under any NRC contract without the approval of SB/DFS. Timely receipt of properly completed security applications is a contract requirement. Failure of the contractor to comply with this condition within the ten work-day period may be a basis to void the notice of selection. In that event, the Government may select another firm for award. When an individual receives final access, the individual will be subject to a reinvestigation every 10 years.

The contractor shall submit a completed security forms packet, including the SF-86, "Questionnaire for National Security Positions," and fingerprint charts, through the Project Officer to the NRC SB/DFS for review and favorable adjudication, prior to the individual performing work under this contract. The contractor shall assure that all forms are accurate, complete, and legible (except for Part 2 of the questionnaire, which is required to be completed in private and submitted by the individual to the contractor in a sealed envelope), as set forth in MD 12.3. Based on SB review of the applicant's security forms and/or the receipt of adverse information by NRC, the individual may be denied access to NRC facilities, sensitive information technology systems or data until a final determination is made of his/her eligibility under the provisions of MD 12.3. Any questions regarding the individual's eligibility for IT Level II approval will be resolved in accordance with the due process procedures set forth in MD 12.3 and E.O. 12968.

In accordance with NRCAR 2052.204.70 "Security," IT Level II contractors shall be subject to the attached NRC Form 187 (See Section J for List of Attachments) which furnishes the basis for providing security requirements to

prime contractors, subcontractors or others (e.g. bidders) who have or may have an NRC contractual relationship which requires access to or operation of agency sensitive information technology systems or remote development and/or analysis of sensitive information technology systems or data or other access to such systems or data; access on a continuing basis (in excess of 30 days) to NRC Headquarters controlled buildings; or otherwise requires issuance of an NRC badge.

CANCELLATION OR TERMINATION OF IT ACCESS/REQUEST

When a request for investigation is to be withdrawn or canceled, the contractor shall immediately notify the Project Officer by telephone in order that he/she will immediately contact the SB/DFS so that the investigation may be promptly discontinued. The notification shall contain the full name of the individual, and the date of the request. Telephone notifications must be promptly confirmed in writing to the Project Officer who will forward the confirmation via email to the SB/DFS. Additionally, SB/DFS must be immediately notified when an individual no longer requires access to NRC sensitive automated information technology systems or data; including the voluntary or involuntary separation of employment of an individual who has been approved for or is being processed for access under the NRC "Personnel Security Program."

D.5 SECURITY REQUIREMENTS FOR BUILDING ACCESS APPROVAL (MARCH 2006)

The contractor shall ensure that all its employees, including any subcontractor employees and any subsequent new employees who are assigned to perform the work herein, are approved by the Government for building access. Timely receipt of properly completed security applications is a contract requirement. Failure of the contractor to comply with this condition within the ten work-day period may be a basis to void the notice of selection. In that event, the Government may select another firm for award.

A contractor employee shall not have access to NRC facilities until he/she is approved by the Security Branch, Division of Facilities and Security (SB/DFS). Temporary access may be approved based on a favorable adjudication of their security forms. Final access will be approved based on favorably adjudicated background checks by the General Services Administration in accordance with the procedures found in NRC Management Directive 12.3, Part I. However, temporary access authorization approval will be revoked and the employee may subsequently be removed from the contract in the event the employee's investigation cannot be favorably adjudicated. Such employee will not be authorized to work under any NRC contract without the approval of SB/DFS. When an individual receives final access, the individual will be subject to a reinvestigation every five years.

The Government shall have and exercise full and complete control over granting, denying, withholding, or terminating building access approvals for individuals performing work under this contract. *Individuals performing work under this contract for a period of 180 days or more* shall be required to complete and submit to the contractor representative an acceptable *OPM Form 85P (Questionnaire for Public Trust Positions)*, and two FD-258 (Fingerprint Charts). Non-U.S. citizens must provide official documentation to the DFS/SB, as proof of their legal residency. This documentation can be a Permanent Resident Card, Temporary Work Visa, Employment Authorization Card, or other official documentation issued by the U. S. Citizenship and Immigration Services. Any applicant with less than two years residency in the U. S. will not be approved for building access. The contractor representative will submit the documents to the Project Officer who will give them to the SB/DFS. SB/DFS may, among other things, grant or deny temporary unescorted building access approval to an individual based upon its review of the information contained in the *OPM Form 85P*. Also, in the exercise of its authority, GSA may, among other things, grant or deny permanent building access approval based on the results of its investigation and adjudication guidelines. This submittal requirement also applies to the officers of the firm who, for any reason, may visit the work sites for an extended period of time during the term of the contract. In the event that SB/DFS and GSA are unable to grant a temporary or permanent building access approval, to any individual performing work under this contract, the contractor is responsible for assigning another individual to perform the necessary function without any delay in the contract's performance schedule, or without adverse impact to any other terms or conditions of the contract. The contractor is responsible for informing those affected by this procedure of the required building access approval process (i.e., temporary and permanent determinations), and the possibility that individuals may be required to wait until permanent building access approvals are granted before beginning work in NRC's buildings.

The contractor will immediately notify the Project Officer when a contractor employee terminates. The Project Officer will immediately notify SB/DFS (via e-mail) when a contractor employee no longer requires building access and return any NRC issued badges to the SB/DFS within three days after their termination.

D.6 SITE ACCESS BADGE REQUIREMENT

During the life of this contract, the rights of ingress and egress for contractor personnel must be made available as required. In this regard, all contractor personnel whose duties under this contract require their presence on-site shall be clearly identifiable by a distinctive badge furnished by the Government. The Project Officer shall assist the contractor in obtaining the badges for the contractor personnel. It is the sole responsibility of the contractor to ensure that each employee has proper identification at all times. All prescribed identification must be immediately delivered to the Security Office for cancellation or disposition upon the termination of employment of any contractor personnel. Contractor personnel must have this identification in their possession during on-site performance under this contract. It is the contractor's duty to assure that contractor personnel enter only those work areas necessary for performance of contract work, and to assure the safeguarding of any Government records or data that contractor personnel may come into contact with.

D.7 BADGE REQUIREMENTS FOR UNESCORTED BUILDING ACCESS TO NRC FACILITIES (MARCH 2006)

During the life of this contract, the rights of ingress and egress for contractor personnel must be made available, as required, provided that the individual has been approved for unescorted access after a favorable adjudication from the Security Branch, Division of Facilities and Security (SB/DFS).

In this regard, all contractor personnel whose duties under this contract require their presence on-site shall be clearly identifiable by a distinctive badge furnished by the NRC. The Project Officer shall assist the contractor in obtaining badges for the contractor personnel. All contractor personnel must present two forms of Identity Source Documents (I-9). One of the documents must be a valid picture ID issued by a state or by the Federal Government. Original I-9 documents must be presented in person for certification. A list of acceptable documents can be found at http://www.usdoj.gov/crt/recruit_employ/i9form.pdf. It is the sole responsibility of the contractor to ensure that each employee has a proper NRC-issued identification/badge at all times. All photo-identification badges must be immediately (no later than three days) delivered to SB/DFS for cancellation or disposition upon the termination of employment of any contractor personnel. Contractor personnel must display any NRC issued badge in clear view at all times during on-site performance under this contract. It is the contractor's duty to assure that contractor personnel enter only those work areas necessary for performance of contract work, and to assure the protection of any Government records or data that contractor personnel may come into contact with.

D.8 APPROPRIATE USE OF GOVERNMENT FURNISHED INFORMATION TECHNOLOGY (IT) EQUIPMENT AND/ OR IT SERVICES/ ACCESS (MARCH 2002)

As part of contract performance the NRC may provide the contractor with information technology (IT) equipment and IT services or IT access as identified in the solicitation or subsequently as identified in the contract or delivery order. Government furnished IT equipment, or IT services, or IT access may include but is not limited to computers, copiers, facsimile machines, printers, pagers, software, phones, Internet access and use, and email access and use. The contractor (including the contractor's employees, consultants and subcontractors) shall use the government furnished IT equipment, and / or IT provided services, and/ or IT access solely to perform the necessary efforts required under the contract. The contractor (including the contractor's employees, consultants and subcontractors) are prohibited from engaging or using the government IT equipment and government provided IT services or IT access for any personal use, misuse, abuses or any other unauthorized usage.

The contractor is responsible for monitoring its employees, consultants and subcontractors to ensure that government furnished IT equipment and/ or IT services, and/ or IT access are not being used for personal use, misused or abused. The government reserves the right to withdraw or suspend the use of its government furnished IT equipment, IT services and/ or IT access arising from contractor personal usage, or misuse or abuse; and/ or to disallow any payments associated with contractor (including the contractor's employees, consultants and subcontractors) personal usage, misuses or abuses of IT equipment, IT services and/ or IT access; and/ or to terminate for cause the contract or delivery order arising from violation of this provision.

D.9 SECURITY REQUIREMENTS FOR ACCESS TO CLASSIFIED MATTER OR INFORMATION (FEB 2004)

Performance under this contract will require access to classified matter or information (National Security Information or Restricted Data) in accordance with the attached NRC Form 187 (See List of Attachments). Prime contractor personnel, subcontractors or others performing work under this contract shall require a "Q" security clearance (allows access to Top Secret, Secret, and Confidential National Security Information and Restricted Data) or a "L" security clearance (allows access to Secret and Confidential National Security Information and/or Confidential Restricted Data).

The proposer/contractor must identify all individuals to work under this contract and propose the type of security clearance required for each. The NRC sponsoring office shall make the final determination of the type of security clearance required for all individuals working under this contract.

Such contractor personnel shall be subject to the NRC contractor personnel security requirements of NRC Management Directive (MD) 12.3, Part I and 10 CFR Part 10.11, which is hereby incorporated by reference and made a part of this contract as though fully set forth herein, and will require a favorably adjudicated Single Scope Background Investigation (SSBI) for "Q" clearances or a favorably adjudicated Limited Background Investigation (LBI) for "L" clearances.

A contractor employee shall not have access to classified information until he/she is granted a security clearance by the Security Branch, Division of Facilities and Security (SB/DFS), based on a favorably adjudicated investigation. In the event the contractor employee's investigation cannot be favorably adjudicated, their interim approval could possibly be revoked and the individual could be subsequently removed from the contract. The individual will be subject to a reinvestigation every five years for "Q" clearances and every ten years for "L" clearances.

The contractor shall submit a completed security forms packet, including the SF-86, "Questionnaire for National Security Positions," and fingerprint charts, through the Project Officer to SB/DFS for review and submission to the Office of Personnel Management for investigation. The individual may not work under this contract until SB has granted them the appropriate security clearance, read, understand, and sign the SF 312, "Classified Information Nondisclosure Agreement." The contractor shall assure that all forms are accurate, complete, and legible (except for Part 2 of the questionnaire, which is required to be completed in private and submitted by the individual to the contractor in a sealed envelope), as set forth in MD 12.3. Based on SB review of the applicant's investigation, the individual may be denied his/her security clearance in accordance with the due process procedures set forth in MD 12.3 Exhibit 1, E. O. 12968, and 10 CFR Part 10.11.

In accordance with NRCAR 2052.204.70 cleared contractors shall be subject to the attached NRC Form 187 (See Section J for List of Attachments) which furnishes the basis for providing security requirements to prime contractors, subcontractors or others (e.g., bidders) who have or may have an NRC contractual relationship which requires access to classified information; access on a continuing basis (in excess of 30 days) to NRC Headquarters controlled buildings; or otherwise requires NRC photo identification or card-key badges.

D.10 NRC INFORMATION TECHNOLOGY SECURITY TRAINING (AUG 2003)

NRC contractors shall ensure that their employees, consultants, and subcontractors with access to the agency's information technology (IT) equipment and/or IT services complete NRC's online initial and refresher IT security training requirements to ensure that their knowledge of IT threats, vulnerabilities, and associated countermeasures remains current. Both the initial and refresher IT security training courses generally last an hour or less and can be taken during the employee's regularly scheduled work day.

Contractor employees, consultants, and subcontractors shall complete the NRC's online, "Computer Security Awareness" course on the same day that they receive access to the agency's IT equipment and/or services, as their first action using the equipment/service. For those contractor employees, consultants, and subcontractors who are already working under this contract, the on-line training must be completed in accordance with agency Network Announcements issued throughout the year 2003 within three weeks of issuance of this modification.

Contractor employees, consultants, and subcontractors who have been granted access to NRC information technology equipment and/or IT services must continue to take IT security refresher training offered online by the

NRC throughout the term of the contract. Contractor employees will receive notice of NRC's online IT security refresher training requirements through agency-wide notices.

The NRC reserves the right to deny or withdraw Contractor use or access to NRC IT equipment and/or services, and/or take other appropriate contract administrative actions (e.g., disallow costs, terminate for cause) should the Contractor violate the Contractor's responsibility under this clause.

D.11 CONTRACTOR ORGANIZATIONAL CONFLICTS OF INTEREST

(a) Purpose. The primary purpose of this clause is to aid in ensuring that the contractor:

(1) Is not placed in a conflicting role because of current or planned interests (financial, contractual, organizational, or otherwise) which relate to the work under this contract; and

(2) Does not obtain an unfair competitive advantage over other parties by virtue of its performance of this contract.

(b) Scope. The restrictions described apply to performance or participation by the contractor, as defined in 48 CFR 2009.570- 2 in the activities covered by this clause.

(c) Work for others.

(1) Notwithstanding any other provision of this contract, during the term of this contract the contractor agrees to forgo entering into consulting or other contractual arrangements with any firm or organization, the result of which may give rise to a conflict of interest with respect to the work being performed under this contract. The contractor shall ensure that all employees under this contract abide by the provision of this clause. If the contractor has reason to believe with respect to itself or any employee that any proposed consultant or other contractual arrangement with any firm or organization may involve a potential conflict of interest, the contractor shall obtain the written approval of the contracting officer before the execution of such contractual arrangement.

(2) The contractor may not represent, assist, or otherwise support an NRC licensee or applicant undergoing an NRC audit, inspection, or review where the activities that are the subject of the audit, inspection or review are the same as or substantially similar to the services within the scope of this contract (or task order as appropriate), except where the NRC licensee or applicant requires the contractor's support to explain or defend the contractor's prior work for the utility or other entity which NRC questions.

(3) When the contractor performs work for the NRC under this contract at any NRC licensee or applicant site, the contractor shall neither solicit nor perform work in the same or similar technical area for that licensee or applicant organization for a period commencing with the award of the task order or beginning of work on the site (if not a task order contract) and ending one year after completion of all work under the associated task order, or last time at the site (if not a task order contract).

(4) When the contractor performs work for the NRC under this contract at any NRC licensee or applicant site,

(i) The contractor may not solicit work at that site for that licensee or applicant during the period of performance of the task order or the contract, as appropriate.

(ii) The contractor may not perform work at that site for that licensee or applicant during the period of performance of the task order or the contract, as appropriate, and for one year thereafter.

(iii) Notwithstanding the foregoing, the contracting officer may authorize the contractor to solicit or perform this type of work (except work in the same or similar technical area) if the contracting officer determines that the situation will not pose a potential for technical bias or unfair competitive advantage.

(d) Disclosure after award.

(1) The contractor warrants that to the best of its knowledge and belief, and except as otherwise set forth in this contract, it does not have any organizational conflicts of interest as defined in 48 CFR 2009.570-2.

(2) The contractor agrees that, if after award, it discovers organizational conflicts of interest with respect to this contract, it shall make an immediate and full disclosure in writing to the contracting officer. This statement must include a description of the action which the contractor has taken or proposes to take to avoid or mitigate such conflicts. The NRC may, however, terminate the contract if termination is in the best interest of the government.

(3) It is recognized that the scope of work of a task-order-type contract necessarily encompasses a broad spectrum of activities. Consequently, if this is a task-order-type contract, the contractor agrees that it will disclose all proposed new work involving NRC licensees or applicants which comes within the scope of work of the underlying contract. Further, if this contract involves work at a licensee or applicant site, the contractor agrees to exercise diligence to discover and disclose any new work at that licensee or applicant site. This disclosure must be made before the submission of a bid or proposal to the utility or other regulated entity and must be received by the NRC at least 15 days before the proposed award date in any event, unless a written justification demonstrating urgency and due diligence to discover and disclose is provided by the contractor and approved by the contracting officer. The disclosure must include the statement of work, the dollar value of the proposed contract, and any other documents that are needed to fully describe the proposed work for the regulated utility or other regulated entity. NRC may deny approval of the disclosed work only when the NRC has issued a task order which includes the technical area and, if site-specific, the site, or has plans to issue a task order which includes the technical area and, if site-specific, the site, or when the work violates paragraphs (c)(2), (c)(3) or (c)(4) of this section.

(e) Access to and use of information.

(1) If in the performance of this contract, the contractor obtains access to information, such as NRC plans, policies, reports, studies, financial plans, internal data protected by the Privacy Act of 1974 (5 U.S.C. Section 552a (1988)), or the Freedom of Information Act (5 U.S.C. Section 552 (1986)), the contractor agrees not to:

(i) Use this information for any private purpose until the information has been released to the public;

(ii) Compete for work for the Commission based on the information for a period of six months after either the completion of this contract or the release of the information to the public, whichever is first;

(iii) Submit an unsolicited proposal to the Government based on the information until one year after the release of the information to the public; or

(iv) Release the information without prior written approval by the contracting officer unless the information has previously been released to the public by the NRC.

(2) In addition, the contractor agrees that, to the extent it receives or is given access to proprietary data, data protected by the Privacy Act of 1974 (5 U.S.C. section 552a (1988)), or the Freedom of Information Act (5 U.S.C. section 552 (1986)), or other confidential or privileged technical, business, or financial information under this contract, the contractor shall treat the information in accordance with restrictions placed on use of the information.

(3) Subject to patent and security provisions of this contract, the contractor shall have the right to use technical data it produces under this contract for private purposes provided that all requirements of this contract have been met.

(f) Subcontracts. Except as provided in 48 CFR 2009.570-2, the contractor shall include this clause, including this paragraph, in subcontracts of any tier. The terms contract, contractor, and contracting officer, must be appropriately modified to preserve the Government's rights.

(g) Remedies. For breach of any of the above restrictions, or for intentional nondisclosure or misrepresentation of any relevant interest required to be disclosed concerning this contract or for such erroneous representations that necessarily imply bad faith, the Government may terminate the contract for default, disqualify the contractor from subsequent contractual efforts, and pursue other remedies permitted by law or this contract.

(h) Waiver. A request for waiver under this clause must be directed in writing to the contracting officer in accordance with the procedures outlined in 48 CFR 2009.570-9.

(i) Follow-on effort. The contractor shall be ineligible to participate in NRC contracts, subcontracts, or proposals therefore (solicited or unsolicited), which stem directly from the contractor's performance of work under this contract.

Furthermore, unless so directed in writing by the contracting officer, the contractor may not perform any technical consulting or management support services work or evaluation activities under this contract on any of its products or services or the products or services of another firm if the contractor has been substantially involved in the development or marketing of the products or services.

(1) If the contractor, under this contract, prepares a complete or essentially complete statement of work or specifications, the contractor is not eligible to perform or participate in the initial contractual effort which is based on the statement of work or specifications. The contractor may not incorporate its products or services in the statement of work or specifications unless so directed in writing by the contracting officer, in which case the restrictions in this paragraph do not apply.

(2) Nothing in this paragraph precludes the contractor from offering or selling its standard commercial items to the Government.

D.12 ADDITIONAL ORGANIZATIONAL CONFLICT OF INTEREST INFORMATION AND REPRESENTATION

This order for CONSOLIDATED INFORMATION SYSTEM SECURITY SERVICES (CISSS) is subject to the requirements and compliance with the Nuclear Regulatory Commission Acquisition Regulations (NRCAR) on Organizational Conflicts of Interest (OCOI) contained at 48 C.F.R Chapter 20, Subpart 2009.5; the NRCAR 48 C.F.R 2052.209-71, OCOI representation requirements; and NRCAR 48 C.F.R 2052.209-72 Contractor OCOI terms and conditions. In order to assist the Contractor and its subcontractors in providing the required C.F.R 2052.209-71 OCOI representation and to insure that an actual OCOI does not exist the following relevant information is provided:

Consistent with 48 C.F.R 2052.209-71 OCOI representation clause, prior to commencement of activities related to the performance of work or task orders under this effort, the Contractor shall provide a written representation that the Contractor and any of its subcontractors have no financial business or contractual relationship with NRC contractor and or NRC subcontractors that are engaged in maintenance or development of NRC systems. If any financial business or contractual relationship is found to exist between the Contractor or the Contractor's subcontractors and NRC prime or subcontractors performing maintenance or development, the Contractor will immediately notify the Contracting Officer. This notification shall detail the relationship, provide an explanation of the nature of the relationship, and provide copies of the contracts or financial instruments for OCOI review by the NRC.

D.13 CURRENT/FORMER AGENCY EMPLOYEE INVOLVEMENT (OCT 1999)

(a) The following representation is required by the NRC Acquisition Regulation 2009.105-70(b). It is not NRC policy to encourage offerors and contractors to propose current/former agency employees to perform work under NRC contracts and as set forth in the above cited provision, the use of such employees may, under certain conditions, adversely affect NRC's consideration of non-competitive proposals and task orders.

(b) There () are () are no current/former NRC employees (including special Government employees performing services as experts, advisors, consultants, or members of advisory committees) who have been or will be involved, directly or indirectly, in developing the offer, or in negotiating on behalf of the offeror, or in managing, administering, or performing any contract, consultant agreement, or subcontract resulting from this offer. For each individual so identified, the Technical and Management proposal must contain, as a separate attachment, the name of the individual, the individual's title while employed by the NRC, the date individual left NRC, and a brief description of the individual's role under this proposal.

D.14 TASK ORDER PROCEDURES (OCT 1999)

(a) Task order request for proposal. When a requirement within the scope of work for this contract is identified, the contracting officer shall transmit to the contractor a Task Order Request for Proposal (TORFP) which may include the following, as appropriate:

- (1) Scope of work/meetings/travel and deliverables;
- (2) Reporting requirements;

(3) Period of performance - place of performance;

(4) Applicable special provisions;

(5) Technical skills required; and

(6) Estimated level of effort.

(b) Task order technical proposal. By the date specified in the TORFP, the contractor shall deliver to the contracting officer a written or verbal (as specified in the TORFP technical proposal submittal instructions) technical proposal that provides the technical information required by the TORFP.

(c) Cost proposal. The contractor's cost proposal for each task order must be fully supported by cost and pricing data adequate to establish the reasonableness of the proposed amounts. When the contractor's estimated cost for the proposed task order exceeds \$100,000 and the period of performance exceeds six months, the contractor may be required to submit a Contractor Spending Plan (CSP) as part of its cost proposal. The TORP indicates if a CSP is required.

(d) Task order award. The contractor shall perform all work described in definitized task orders issued by the contracting officer. Definitized task orders include the following:

- (1) Statement of work/meetings/travel and deliverables;
- (2) Reporting requirements;
- (3) Period of performance;
- (4) Key personnel;
- (5) Applicable special provisions; and
- (6) Total task order amount including any fixed fee.

D.15 ACCELERATED TASK ORDER PROCEDURES (JAN 1993)

(a) The NRC may require the contractor to begin work before receiving a definitized task order from the contracting officer. Accordingly, when the contracting officer verbally authorizes the work, the contractor shall proceed with performance of the task order subject to the monetary limitation established for the task order by the contracting officer.

(b) When this accelerated procedure is employed by the NRC, the contractor agrees to begin promptly negotiating with the contracting officer the terms of the definitive task order and agrees to submit a cost proposal with supporting cost or pricing data. If agreement on a definitized task order is not reached by the target date mutually agreed upon by the contractor and contracting officer, the contracting officer may determine a reasonable price and/or fee in accordance with Subpart 15.8 and Part 31 of the FAR, subject to contractor appeal as provided in 52.233-1, Disputes. In any event, the contractor shall proceed with completion of the task order, subject only to the monetary limitation established by the contracting officer and the terms and conditions of the basic contract.

D.16 PROJECT OFFICER AUTHORITY

(a) The contracting officer's authorized representative hereinafter referred to as the project officer for this contract is:

Name:	Carl Konzman
Address:	U.S. Nuclear Regulatory Commission Mailstop: T-6-F-41 11545 Rockville Pike Washington, DC 20555
Email:	<u>CXK1@NRC.GOV</u>
Telephone Number:	301-415-0592

(b) Performance of the work under this order is subject to the technical direction of the NRC Project Officer. The term "technical direction" is defined to include the following:

- 1) Technical direction to the Contractor which shifts work emphasis between areas of work or tasks, fills in details, or otherwise serves to accomplish the contractual statement of work.
 - 2) Provide advice and guidance to the Contractor in the preparation of drawings, specifications, or technical portions of the work description.
 - 3) Review and, where required by the order, approves technical reports, drawings, specifications, and technical information to be delivered by the Contractor to the Government under the order.
- (c) Technical direction must be within the general statement of work stated in the order. The Project Officer does not have the authority to and may not issue any technical direction which:
- 1) Constitutes an assignment of work outside the general scope of the order.
 - 2) Constitutes a change as defined in the "Changes" clause of the contract/order.
 - 3) In any way causes an increase or decrease in the total estimated order cost, the fixed fee, if any, or the time required for order performance.
 - 4) Changes any of the expressed terms, conditions, or specifications of the order.
 - 5) Terminates the order, settles any claim or dispute arising under the order, or issues any unilateral directive whatever.
- (d) The Contractor shall proceed promptly with the performance of technical directions duly issued by the Project Officer in the manner prescribed by this clause and within the Project Officer's authority under the provisions of this clause.
- (e) If, in the opinion of the Contractor, any instruction or direction issued by the Project Officer is within one of the categories as defined in paragraph c) of this section, the Contractor may not proceed but shall notify the Contracting Officer in writing within five (5) working days after the receipt of any instruction or direction and shall request the Contracting Officer to modify the order accordingly. Upon receiving the notification from the Contractor, the Contracting Officer shall issue an appropriate modification or advise the Contractor in writing that, in the Contracting Officer's opinion, the technical direction is within the scope of this article and does not constitute a change under the "Changes" clause.
- (f) Any unauthorized commitment or direction issued by the Project Officer may result in an unnecessary delay in the Contractor's performance and may even result in the Contractor expending funds for unallowable costs under the order.
- (g) A failure of the parties to agree upon the nature of the instruction or direction or upon the order action to be taken with respect thereto is subject to 52.233 1 Disputes.
- (h) In addition to providing technical direction as defined in paragraph (b) of the section, the Project Officer shall:
- 1) Monitor the Contractor's technical progress, including surveillance and assessment of performance, and recommend to the Contracting Officer changes in requirements.
 - 2) Assist the Contractor in the resolution of technical problems encountered during performance.
 - 3) Review all costs requested for reimbursement by the Contractor and submit to the Contracting Officer recommendations for approval, disapproval, or suspension of payment for supplies and services required under this order.
 - 4) Assist the Contractor in obtaining the badges for the Contractor personnel.
 - 5) Immediately notify the Personnel Security Branch, Division of Facilities and Security (PERSEC/DFS) (via e-mail) when a Contractor employee no longer requires access authorization and return the individual's badge to PERSEC/DFS within three days after their termination.

D.17 KEY PERSONNEL (JAN 1993)

- (a) The following individuals are considered to be essential to the successful performance of the work hereunder:

[REDACTED]

[REDACTED]

The contractor agrees that personnel may not be removed from the contract work or replaced without compliance with paragraphs (b) and (c) of this section.

(b) If one or more of the key personnel, for whatever reason, becomes, or is expected to become, unavailable for work under this contract for a continuous period exceeding 30 work days, or is expected to devote substantially less effort to the work than indicated in the proposal or initially anticipated, the contractor shall immediately notify the contracting officer and shall, subject to the concurrence of the contracting officer, promptly replace the personnel with personnel of at least substantially equal ability and qualifications.

(c) Each request for approval of substitutions must be in writing and contain a detailed explanation of the circumstances necessitating the proposed substitutions. The request must also contain a complete resume for the proposed substitute and other information requested or needed by the contracting officer to evaluate the proposed substitution. The contracting officer and the project officer shall evaluate the contractor's request and the contracting officer shall promptly notify the contractor of his or her decision in writing.

(d) If the contracting officer determines that suitable and timely replacement of key personnel who have been reassigned, terminated, or have otherwise become unavailable for the contract work is not reasonably forthcoming, or that the resultant reduction of productive effort would be so substantial as to impair the successful completion of the contract or the service order, the contract may be terminated by the contracting officer for default or for the convenience of the Government, as appropriate. If the contracting officer finds the contractor at fault for the condition, the contract price or fixed fee may be equitably adjusted downward to compensate the Government for any resultant delay, loss, or damage.

D.18 GOVERNMENT FURNISHED EQUIPMENT/PROPERTY - NONE PROVIDED (JUN 1988)

The Government will not provide any equipment/property under this contract.

D.19 SEAT BELTS

Contractors, subcontractors, and grantees, are encouraged to adopt and enforce on-the-job seat belt policies and programs for their employees when operating company-owned, rented, or personally owned vehicles.

D.20 COMPLIANCE WITH U.S. IMMIGRATION LAWS AND REGULATIONS

NRC contractors are responsible to ensure that their alien personnel are not in violation of United States Immigration and Naturalization (INS) laws and regulations, including employment authorization documents and visa requirements. Each alien employee of the Contractor must be lawfully admitted for permanent residence as evidenced by Alien Registration Receipt Card Form 1-151 or must present other evidence from the Immigration and Naturalization Services that employment will not affect his/her immigration status. The INS Office of Business Liaison (OBL) provides information to contractors to help them understand the employment eligibility verification process for non-US citizens. This information can be found on the INS website, <http://www.ins.usdoj.gov/graphics/services/employerinfo/index.htm#obl>.

The NRC reserves the right to deny or withdraw Contractor use or access to NRC facilities or its equipment/services, and/or take any number of contract administrative actions (e.g., disallow costs, terminate for cause) should the Contractor violate the Contractor's responsibility under this clause.

D.21 PAYMENT FOR OVERTIME PREMIUMS

No overtime premiums are authorized for the performance of this contract.

D.22 AUTHORITY TO USE GOVERNMENT PROVIDED SPACE AT NRC HEADQUARTERS

Prior to occupying any government provided space at the NRC Headquarters in Rockville Maryland, the Contractor shall obtain written authorization to occupy specifically designated government space via the NRC Project Officer

from the Chief, Space Planning and property Management Branch, Division Of Facilities and Security. Failure to obtain this prior authorization may result in one or a combination of the following remedies as deemed appropriate by the Contracting Officer:

1. Rental charge for the space occupied to be deducted from invoice amount due the Contractor
2. Removal from the space occupied
3. Contract Termination

D.23 BILLING INSTRUCTIONS FOR T&M CONTRACTS

General: The Contractor shall prepare vouchers/invoices for reimbursement of costs in the manner and format described herein or a similar format. **FAILURE TO SUBMIT VOUCHERS/INVOICES IN ACCORDANCE WITH THESE INSTRUCTIONS WILL RESULT IN REJECTION OF THE VOUCHER/INVOICE AS IMPROPER.**

Number of Copies: An original and three copies, including supporting documentation shall be submitted. A copy of all supporting documents must be attached to each copy of your voucher/invoice. Failure to submit all the required copies will result in rejection of the voucher/invoice as improper.

Designated Agency Billing Office: Vouchers/invoices shall be submitted to the following address:

U.S. Nuclear Regulatory Commission
Division of Contracts
Mail Stop T-7-I-2
Washington, D.C. 20555

HAND DELIVERY OF VOUCHERS/INVOICES IS DISCOURAGED AND WILL NOT EXPEDITE PROCESSING BY NRC. However, should you choose to deliver vouchers/invoices by hand, including delivery by any express mail services or special delivery services which use a courier or other person to deliver the voucher/invoice in person to the NRC, such vouchers/invoices must be addressed to the above Designated Agency Billing Office and will only be accepted at the following location:

U.S. Nuclear Regulatory Commission
One White Flint North
11555 Rockville Pike - Mail Room
Rockville, MD 20852

HAND-CARRIED SUBMISSIONS WILL NOT BE ACCEPTED AT OTHER THAN THE ABOVE ADDRESS.

Note that the official receipt date for hand-delivered vouchers/invoices will be the date it is received by the official agency billing office in the Division of Contracts and Property Management.

Agency Payment Office: Payment will be made by the following office:

U.S. Nuclear Regulatory Commission
Division of Accounting and Finance GOV/COMM
Mail Stop T-9-H4
Washington, DC 20555

Frequency: The Contractor shall submit claims for reimbursement once each month, unless otherwise authorized by the Contracting Officer.

Format: Claims should be submitted in the format depicted on the attached sample form entitled "Voucher/Invoice for Purchases and Services Other Than Personal" (see below) or a similar format for each task order. *For each deliverable or annual service associated with the task order, costs should be itemized by labor category, hours and associated labor rate.* **THE SAMPLE FORMAT IS PROVIDED FOR GUIDANCE ONLY AND IS NOT REQUIRED FOR SUBMISSION OF A VOUCHER/INVOICE. ALTERNATE FORMATS ARE PERMISSIBLE PROVIDED ALL REQUIREMENTS OF THE BILLING INSTRUCTIONS ARE ADDRESSED.**

Billing of Costs after Expiration of Contract/Task Order: If the costs are incurred during the contract/task order period and claimed after the contract/task order has expired, the period during which these costs were incurred must be cited. To be considered a proper voucher/invoice, the Contractor shall clearly mark it "EXPIRATION VOUCHER" or "EXPIRATION INVOICE".

Currency: Billings may be expressed in the currency normally used by the Contractor in maintaining his accounting records; payments will be made in that currency. However, the U.S. dollar equivalent for all vouchers/invoices paid under the purchase order may not exceed the total U.S. dollars authorized in the contract/task order.

INVOICE/VOUCHER FOR PURCHASES AND SERVICES OTHER THAN PERSONAL

Official Agency Billing Office
U.S. Nuclear Regulatory Commission
Division of Contracts and Property
Management MS: T-7-I2
Washington, DC 20555-0001

(a) Contract/Task Order No:

(b) Voucher/Invoice No:

(c) Date of Voucher/Invoice:

Payee's Name and Address

(d) Individual to Contact Regarding Voucher/Invoice
Name: Telephone No:

(e) This voucher/invoice represents reimbursable costs for the billing period
_____ to _____

	<u>Current Period</u>	<u>Amount Billed</u>	<u>Cumulative</u>
<u>Direct Costs:</u>			
Deliverable Title:			
(1) Direct Labor*	\$ _____		\$ _____
(2) Travel*	\$ _____		\$ _____
Total Direct Costs:	\$ _____		\$ _____
Task Order:			
(1) Direct Labor*	\$ _____		\$ _____
(2) Travel*	\$ _____		\$ _____
Total Direct Costs:	\$ _____		\$ _____

The Contractor shall submit as an attachment to its invoice/voucher cover sheet a listing of labor categories, hours billed, fixed hourly rates, total dollars, and cumulative hours billed to date under each labor category *for each deliverable or annual service*, authorized under the contract/task order for each of the activities to be performed under the task order. In addition, the Contractor shall include travel costs incurred with the required supporting documentation, as well as, the cumulative total of travel costs billed to date by activity.

The policies, procedures, and criteria of the NRC Security Program, NRCMD 12, apply to performance of this contract, subcontract or other activity.

CONTRACT SECURITY AND/OR CLASSIFICATION REQUIREMENTS

COMPLETE CLASSIFIED ITEMS BY SEPARATE CORRESPONDENCE

1. CONTRACTOR NAME AND ADDRESS

A. CONTRACT NUMBER FOR COMMERCIAL CONTRACTS OR JOB CODE FOR DOE PROJECTS (Prime contract number must be shown for all subcontracts.)

B. PROJECTED
START DATE

C. PROJECTED
COMPLETION DATE

2. TYPE OF SUBMISSION



A. ORIGINAL



B. REVISED (Supersedes all previous submissions)



C. OTHER (Specify)

3. FOR FOLLOW-ON CONTRACT, ENTER PRECEDING CONTRACT NUMBER AND PROJECTED COMPLETION DATE

A. DOES NOT APPLY



B. CONTRACT NUMBER

DATE

4. PROJECT TITLE AND OTHER IDENTIFYING INFORMATION

Consolidated Information Systems Security Services Contract

5. PERFORMANCE WILL REQUIRE

A. ACCESS TO CLASSIFIED MATTER OR CLASSIFIED INFORMATION



YES (If "YES," answer 1-7 below)



NO (If "NO," proceed to 5.C.)

NOT
APPLICABLE

NATIONAL SECURITY

RESTRICTED DATA

SECRET

CONFIDENTIAL

SECRET

CONFIDENTIAL

1. ACCESS TO FOREIGN INTELLIGENCE INFORMATION



2. RECEIPT, STORAGE, OR OTHER SAFEGUARDING OF CLASSIFIED MATTER. (See 5.B.)



3. GENERATION OF CLASSIFIED MATTER.



4. ACCESS TO CRYPTOGRAPHIC MATERIAL OR OTHER CLASSIFIED COMSEC INFORMATION.



5. ACCESS TO CLASSIFIED MATTER OR CLASSIFIED INFORMATION PROCESSED BY ANOTHER AGENCY.



6. CLASSIFIED USE OF AN INFORMATION TECHNOLOGY PROCESSING SYSTEM.



7. OTHER (Specify)



B. IS FACILITY CLEARANCE REQUIRED?



YES



NO

C. ☐ UNESCORTED ACCESS IS REQUIRED TO PROTECTED AND VITAL AREAS OF NUCLEAR POWER PLANTS.

D. ☒ ACCESS IS REQUIRED TO UNCLASSIFIED SAFEGUARDS INFORMATION.

E. ☒ ACCESS IS REQUIRED TO SENSITIVE IT SYSTEMS AND DATA.

F. ☒ UNESCORTED ACCESS TO NRC HEADQUARTERS BUILDING.

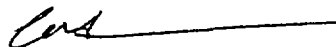
FOR PROCEDURES AND REQUIREMENTS ON PROVIDING TEMPORARY AND FINAL APPROVAL FOR UNESCORTED ACCESS, REFER TO NRCMD 12.

6. INFORMATION PERTAINING TO THESE REQUIREMENTS OR THIS PROJECT, EVEN THOUGH SUCH INFORMATION IS CONSIDERED UNCLASSIFIED, SHALL NOT BE RELEASED FOR DISSEMINATION EXCEPT AS APPROVED BY:

NAME AND TITLE

Carl Konzman, Senior Project Manager

SIGNATURE



DATE

01/24/06

7. CLASSIFICATION GUIDANCE

NATURE OF CLASSIFIED GUIDANCE IDENTIFICATION OF CLASSIFICATION GUIDES

Management Directive 12.3

Management Directive 12.6

~~10 CFR 73.24~~ MD 12.2

Applicable Nat'l Guidance

DE-SGI-1

8. CLASSIFIED REVIEW OF CONTRACTOR / SUBCONTRACTOR REPORT(S) AND OTHER DOCUMENTS WILL BE CONDUCTED BY:



AUTHORIZED CLASSIFIER (Name and Title)



DIVISION OF FACILITIES AND SECURITY

No See Note
Lynn Silvius, Chief, Information Security

Section, NSIR An OIS person to be named and trained.

9. REQUIRED DISTRIBUTION OF NRC FORM 187 Check appropriate box(es)



SPONSORING NRC OFFICE OR DIVISION (Item 10A)



DIVISION OF CONTRACTS AND PROPERTY MANAGEMENT



DIVISION OF FACILITIES AND SECURITY (Item 10B)



CONTRACTOR (Item 1)



SECURITY/CLASSIFICATION REQUIREMENTS FOR SUBCONTRACTS RESULTING FROM THIS CONTRACT WILL BE APPROVED BY THE OFFICIALS NAMED IN ITEMS 10B AND 10C BELOW.

10. APPROVALS

SECURITY/CLASSIFICATION REQUIREMENTS FOR SUBCONTRACTS RESULTING FROM THIS CONTRACT WILL BE APPROVED BY THE OFFICIALS NAMED IN ITEMS 10B AND 10C BELOW.

NAME (Print or type)

SIGNATURE

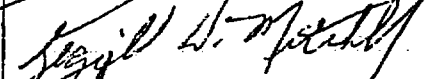
DATE

A. DIRECTOR, OFFICE OR DIVISION

SIGNATURE

DATE

Reginald W. Mitchell



1/24/06

B. DIRECTOR, DIVISION OF FACILITIES AND SECURITY

SIGNATURE

DATE

Sharon D. Stewart



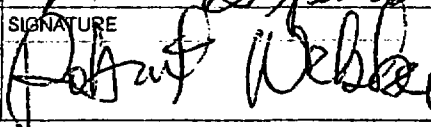
4/21/06

C. DIRECTOR, DIVISION OF CONTRACTS AND PROPERTY MANAGEMENT
(Not applicable to DOE agreements)

SIGNATURE

DATE

Mary Lynn Scott



4/21/06

REMARKS

No classified activities will occur at contractor facilities. All classified activities will occur at NRC owned and controlled government facilities.

SOW ENCLOSURE 2 - MONTHLY PROGRESS REPORT FORMAT

The Monthly Progress Report shall include, at a minimum, the following sections.

I. WORK PROGRESS STATUS BY TASK ORDER

a. General Information/Description

- Task Order Number and Description
- The Job Code Number (JCN) and title
- The NRC Project Officer and telephone number
- NRC Task Order Manager

b. Financial Summary

- Authorized ceiling amount
- Total amount of funds obligated
- The total planned cost incurred for the period, Government fiscal year to date, and cumulative to date
- The total estimated cost for the period, fiscal year to date and cumulative to date
- The total actual cost for the period, fiscal year to date and cumulative to date
- Percent of funds expended against obligated funds

2. SCHEDULE/MILESTONE STATUS

Planned Tasks	Scheduled Completion Date	Revised Completion Date	Actual Completion Date
Provide a brief summary of the work; include any report or travel.	The day, month and year scheduled for completion, or timeframe if a date is not known or projected below.	The revised day, month and year based on a change. The reason for the change must be given in the "Problem/Resolution" section.	The day, month and year all work is actually completed.

3. WORK PERFORMED DURING THE PERIOD

A description of the work performed and accomplished commensurate with the amount of funds expended; i.e., the description should provide the reader with sufficient explanation of the work to justify the amount of expenditures. A description of all deliverable deficiencies encountered during the reporting period with associated corrective actions implemented. A trend analysis of all deficiencies to date (cumulative) shall also be included in the report.

Any travel taken during the reporting period should also be summarized in this section of the report. Each travel summary should identify the persons traveling, the duration of the travel, the purpose of the travel, and any work/accomplishments not reflected elsewhere.

4. PROBLEM/RESOLUTION

- All problems encountered during the period should be clearly and succinctly identified and stated. Then, the resolution or the proposed solution should be briefly described. It should be clearly evident, from a reading of the description, the personnel responsible for solving the problem, should it still exist at the time the report is written.
- Notwithstanding the status of the problem at the time the Monthly Progress Report is written, all problems should be recorded in the "Problem/ Resolution" section of the Monthly Progress Report for documentation/historical purposes. If the problem still exists in a subsequent month, in whole or in part, it should be described as it currently exists; otherwise, it should be deleted from the report.
- Problems or circumstances that require a change in the level of effort/costs, scope, or travel requirements are to be described in the Monthly Progress Reports for documentation purposes, but are to be dealt with separately in a letter addressed to the Project Officer and Contracting Officer.

5. EARNED VALUE MANAGEMENT (EVM) DATA

The Contractor shall report earned value consistent with the Section A-11, Part 7 of the ANSI Standard 748. Schedule variance data submitted shall provide visibility into root causes and establish corrective actions to achieve project completion within established task order schedule. All EVM data shall be provided in tabular and graphical formats to communicate cost variance and schedule status, as well as the technical completion status of the project relative to the Performance Measurement Baseline.

- EVM data shall be collected using 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.**
- The Contractor shall collect and report on each of the following measures:
 - Performance Measurement Baseline (PMB)**
 - Budget Cost of Work Scheduled (BCWS)**
 - Actual Cost of Work Performed (ACWP)**
 - Budgeted Cost of Work Performed (BCWP)**
 - Cost Variance (CV)** – The numerical difference between the earned value (BCWP) and the actual cost (ACWP). $CV = BCWP - ACWP$.
 - Schedule Variance (SV)** - An indicator of how much a program is ahead of or behind schedule. $SV = BCWP - BCWS$.
 - Cost Performance Index (CPI)** – The cost efficiency factor representing the relationship between the actual cost expended and the earned value. $CPI = BCWP/ACWP$.
 - Schedule Performance Index (SPI)** – The planned schedule efficiency factor representing the relationship between the earned value and the initial planned schedule. $SPI = BCWP/BCWS$.
 - Budget at Completion (BAC)** – sum total of the time-phased budget.
 - Estimate to Complete (ETC)** – A calculated value, in dollars or hours, that represents the cost of work required to complete remaining project tasks. $ETC = BAC - BCWP$.
 - Estimate at Complete (EAC)** – A calculated value, in dollars or hours, that represents the projected total final costs of work when completed. $EAC = ACWP + ETC$.
- The Contractor shall calculate Earned value credit as a binary value, with 0 percent being given before task completion and 100 percent given when completion of each work unit is validated. The Contractor shall establish specific measurable exit criteria for each task to simplify tracking of task completion, and thus credit the earned value of the task to the project so that the earned value of the project at any given point in time is obtained by "simple math" rather than by subjective assessment.

6. PLANS FOR NEXT PERIOD

Provide a brief description of the work to be performed and accomplished during the next reporting period. If a milestone is expected to be completed during the next report period, identify this milestone.

SOW ENCLOSURE 3 - RESERVED

(This page left blank intentionally.)

SOW ENCLOSURE 4 - REFERENCES

Applicable Documents to be used as reference when creating documentation to validate compliancy can be located at the following: <http://csrc.nist.gov/publications/index.html>

SOW ENCLOSURE 5 - TERMS AND DEFINITIONS

ISS Program Unclassified:

The Contractor shall utilize the Rational Suite Enterprise in the certification and accreditation of NRC information systems leveraging common security controls and solutions stored and automatically populated for an individual project within the Rational Suite Enterprise.

ISS Program Classified:

The Contractor shall support the NRC staff in the development of hard copy certification and accreditation documentation for DAA review and approval of classified NRC information systems consistent with compartmented and trusted information systems security engineering principles, and in compliance with National Security Systems and Intelligence Systems classified/trusted information systems application development, and security certification and accreditation guidance.

Major Application (MA):

The term "Major Application" means a computerized information system or application that requires special attention to security because of the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. Because of their impact on the agency mission and the information they contain or process, MAs require special management oversight. (See OMB Circular A-130, Appendix III.) For example, an agency wide financial management system containing NRC's official financial records would be an MA. A computer program or a spreadsheet designed to track expenditures against an office budget would not be considered an MA. Similarly, commercial off-the-shelf software products (such as word processing software, electronic mail software, utility software, or general purpose software) would not typically be considered MAs.

General Support System (GSS):

A GSS is an interconnected set of information resources under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, and people. (See OMB Circular A-130, Appendix III.) The mission objective of a GSS is to provide automated information system resources in support of the organizational mission. Typical GSSs are LANs, WANs, servers, and data processing centers.

E-Government (E-Gov):

E-Gov systems consist of a number of externally hosted information system components that consolidate information into a single, trusted information systems framework supporting the six Presidential E-Gov initiatives.

Listed System:

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. The security plan for a listed system will describe those additional security protections and controls. These additional security controls could refer to the use of additional passwords, or the use of additional security technology such as virtual private networks (VPNs), digital signatures, secure Web sites, or other security solutions based on the use of public key infrastructure (PKI) technology. In addition, any system that processes classified information or unclassified Safeguards Information (SGI) that is not a GSS or a MA shall be categorized as a Listed System. An abbreviated security plan format that is compliant with National Institute of Standards and Technology (NIST) security plan guidance is available on the NRC internal Web site.

Other:

If the sponsor for an NRC system does not believe that additional security protections are necessary and the information being processed by the office non-major application is adequately protected by the security provided by the NRC LAN/WAN, such a system shall be categorized as an "Other" system. This categorization assumes that

OIS and the sponsor have first jointly decided that the application is appropriately called a system and is to be included in the NRC master inventory of systems. Systems in the NRC Other category are typically collections of computer-based activities that while focused on a particular mission function or objective do not have the structure, size, data sensitivity, or the mission importance to warrant additional special management attention or additional security controls. An office database system used by multiple individuals to support tracking and analysis of licensee reports may be categorized as "other". It is up to each individual sponsor to determine which office non-major applications should be categorized as Listed Systems, Other systems, or systems that are so small that they will not be categorized as a system. The Security Plan for the NRC LAN/WAN GSS covers all of the NRC systems on the network that are categorized as "Other".

SOW ENCLOSURE 6 - C&A PROCESS AND DELIVERABLES

1.0 ISS PROGRAM UNCLASSIFIED

The Contractor shall utilize the Rational Suite Enterprise in the certification and accreditation of NRC Information systems leveraging common security controls and solutions stored and automatically populated for an individual project within the Rational Suite Enterprise.

1.1 MAJOR APPLICATION

1.1.1 Security Categorization Report

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.

1.1.1.1 Privacy Impact Assessment

The Contractor shall review and propose changes to the NRC completed privacy impact assessments for consistency with Section 208 of the Electronic Government Act, and information obtained during the systems security categorization.

1.1.1.2 Electronic Records Management Disposition

The Contractor shall review and propose changes to the NRC completed electronic records management forms (NRC Form 616 and NRC Form 637) for all NRC IT systems consistent with Code of Federal Regulations Part 36 and OMB Circular A-130, and information obtained during the systems security categorization.

1.1.1.3 E-Authentication Risk Assessments

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.

1.1.2 Risk Assessment

The assessment of risk and the development of system security plans are two important activities in an agency's information security program that directly support security accreditation and are required by the 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 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 risk 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. 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 will 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.

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

1.1.3 Systems Security Plan (SSP)

The security plan shall be developed in accordance with NIST SP 800-53 Recommended Security Controls for Federal Information Systems, NIST SP 800-37 Guide for the Security Certification and Accreditation of Federal Information Systems, and the NRC IT Security Plan Template. The Contractor shall identify within the SSP the necessary security controls required, citing the security controls that are in place, those that are planned, and those that are not applicable.

Where a system relies upon a control that is provided by another system (e.g. the NRC LAN/WAN), the specific control being relied upon shall be noted along with the name of the system providing that control. The Contractor shall trace the security controls to specific documented guidance, NRC policy (e.g., Management Directives), infrastructure policy or procedures.

The system security plan shall be documented in a report that follows the NRC Template for System Security Plan. The report shall be delivered in draft form and then in pre-system ST&E form after NRC comments are incorporated. The NRC IT Security staff review of the draft is required to ensure compliance. The Contractor shall update the system security plan after completion of the ST&E test report to reflect validated in-place and planned controls. The NRC SITSO must approve the final to enable system accreditation.

1.1.3.1 System Security Controls and Security Requirements Support

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

1.1.4 Review, Verification, and Validation of Security Controls and Requirements

The Contractor shall review, verify, and validate all security controls and security requirements and associated technical resolutions, risk mitigation, and implementations contained within various NRC security and systems development documentation or the Rational Suite Enterprise such that confirmation that the system and associated controls are operating as intended.

1.1.5 Systems Security Controls and Security Requirements Test Plan Development Support

The Contractor shall support the NRC staff in the development and documentation of a test plan within the Rational Suite Enterprise that exercises the systems security controls and security requirements and associated technical resolutions, risk mitigation, and implementations such that confirmation that the system and associated controls are operating as intended and in accordance with NIST SP 800-53 Recommended Security Controls for Federal Information Systems, NIST SP 800-37 Guide for the Security Certification and Accreditation of Federal Information Systems, and the NRC System Security Test and Evaluation Plan Template. The Contractor shall provide detailed test procedures to ensure all IT security functional and assurance requirements are fully tested. The procedures shall contain sufficient detail that a technically trained individual not familiar with the system can successfully follow the procedures.

The System Test and Evaluation (ST&E) plan shall identify all testing assumptions, constraints, and dependencies and include a proposed schedule that identifies which personnel, hardware, software, and other requirements that must be met for each portion of the schedule to accomplish full system security testing of all system security functional and assurance requirements where the requirements are not stated as being fulfilled by another system. The following test methods shall be used:

1.1.5.1 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.

1.1.5.2 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. (Example: Observe visitors upon computer room entry in order to verify that all visitation procedures are followed.)

1.1.5.3 Interview

The Contractor will interview personnel to verify the security policies and procedures are understood as implemented and prescribed by governing policies and regulations.

1.1.5.4 Inspection

The Contractor will review and analyze visitor logs to verify all information requested has been entered on the log. (Example: The Contractor shall verify that the visitor's name, signature, organization, reason of visit, arrival and departure date, time, and the escort's name, initials, or signature are included on the log sheets.)

1.1.5.5 Technical Test

The Technical Test verification method shall be used to verify that each implemented control is functioning as intended with the Contractor attempting to access a system by logging on to that system from his workstation (or other device) using an incorrect password to see if the system responds with an error message stating incorrect password or denies access after exceeding the maximum threshold for logon attempts and is directed to call the system administrator to gain access.

Testing requirements that are stated as being fulfilled by another system (provider) shall be accomplished by verifying that the provider system security plan in-place controls meet the requirement.

1.1.6 Review, Verification, and Validation of Security Controls and Requirements Test Plan and Test Plan Execution

The Contractor shall independently review, verify, and validate all systems security test plans and procedures to ensure the accuracy and adequacy of documented test procedures for all systems security controls and security requirements and associated technical resolutions, risk mitigation, and implementations contained within various NRC security and systems development documentation or the Rational Suite Enterprise such that confirmation that the system and associated controls are operating as intended. The Contractor shall update the STE Plan after completion of the system security test and evaluation plan test report to reflect validated information. The NRC Senior IT Security Officer must approve the final to enable system accreditation.

1.1.7 Contingency Plan

The Contractor shall support the NRC staff in the development and documentation of a contingency plan and test procedures within the Rational Suite Enterprise. The System Contingency Plan shall be documented in a report generated from the Rational Suite Enterprise that follows the NRC Template for the System Contingency Plan. The Plan shall be maintained in its hard copy form for contingency execution should the Rational Suite Enterprise or NRC Network Infrastructure be unavailable. The contingency plan shall be developed in accordance with NIST SP 800-34 Contingency Planning Guide for Information Technology Systems, NIST SP 800-37 Guide for the Security Certification and Accreditation of Federal Information Systems, and the NRC Contingency Plan (CP) Template. The Contractor shall provide detailed procedures for the notification and activation phase, recovery operations, and return to normal operations. The procedures shall contain sufficient detail that a technically trained individual not familiar with the system can successfully follow the procedures. The system contingency plan shall also contain sufficient personnel contact information to enable contact at all times, vendor contact information to enable contact at all times, equipment (hardware and software) and specification information to enable reconstitution of the system from scratch, all service level agreements and memoranda of understanding, the IT standard operating procedures for the system, identification of any systems that this system is dependent upon along with references for the applicable contingency plans, references to the emergency management plan and occupant evacuation plan, and references to the appropriate continuity of operations plan.

The System Contingency Plan shall be documented in a report generated from the Rational Suite Enterprise that follows the NRC Template for System Contingency Plan. The report shall be delivered in draft form and then in pre-Test form after NRC comments are incorporated. The NRC IT Security staff review of the draft is required to ensure compliance. The Contractor shall update the system contingency plan after completion of the contingency plan test report to reflect validated information. The NRC Senior IT Security Officer must approve the final version to enable system accreditation.

1.1.8 Contingency Planning Test and Report

The Contractor shall provide expert advice and support during the Contingency Planning Test to ensure test plan documentation is compliant with the System Contingency Plan (CP) that has been approved by the NRC Senior Information Technology Security Officer (SITSO). Testing shall follow the test procedures developed and documented by the Contractor within the Rational Suite Enterprise. The Contractor shall document the testing in a System Contingency Test Report (CP Test Report). The CP Test Report shall be developed in accordance with NIST SP 800-34 Contingency Planning Guide for Information Technology Systems, NIST SP 800-37 Guide for the Security Certification and Accreditation of Federal Information Systems, and the NRC Contingency Test Report Template.

The CP Test shall be documented in a report that follows the NRC Template for NRC Contingency Test Report. The CP Test Report shall identify all testing assumptions, constraints, and dependencies as well as any anomalies, impromptu tests, and deviations encountered during testing. The CP Test Report shall include the actual testing schedule and detailed test results for each test procedure outlining specific errors encountered. The CP Test Report shall include a table of test findings incorporating any test issues and recommendations. The CP Test Report shall identify any problems encountered during testing and identify the resulting action items for the system. The CP Test Report shall be delivered in draft form and then in final form after NRC comments are incorporated. The NRC SITSO must approve the final CP Test Report to enable system accreditation.

1.1.9 Quarterly Penetration and Vulnerability Scanning

The Contractor shall perform quarterly analysis, penetration, vulnerability, configuration, systems integrity, and patch management scans. The Contractor shall identify, analyze, and propose tested corrective actions that address Plan of Action and Milestone (POAM) items as identified by the SITSO, ensure that controls are operating as intended, and assure currency of the systems security posture is consistent with the latest Defense Information Systems Agency (DISA) and Center for Internet Security (CIS) benchmarks and scoring tools available at the time of analysis.

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

1.1.10 Annual Analysis of Systems Documentation, Security Controls, Requirements, and Implementation Status

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

1.1.11 Development, Update and Maintenance of Common Control Sets and Procedures

The Contractor shall develop a standardized set of streamlined security certification and accreditation documentation that focuses on the functional alignment of common security control sets and standard operating procedures for LOW, MODERATE, and HIGH Baseline systems consistent with FISMA, and NIST SP 800-53 that integrate with the NRC Project Management Methodology (PMM) and Enterprise Architecture (EA) within the Rational Suite Enterprise.

1.1.12 Security Engineering, and Common Security Controls Support

The Contractor shall provide Security Engineering support for application development and information systems solution assessment and proposal such that information systems architectures proposed for implementation at the NRC are based on sound security engineering principles and practices. The Contractor shall support the NRC enterprise architecture staff in the development of the security line of business program and documentation, and support the NRC in the assessment, documentation, and implementation of common security solutions OMB information systems security line of business integration.

1.1.13 Security Reporting

In addition to the applicable requirements, the Contractor shall provide a POAM Status Tracking Report, FISMA Compliance and Health Report, Risk and Security Vulnerability Trending Report, Security Scoping and Categorization Report, and Security Costs Report.

1.2 GENERAL SUPPORT SYSTEM

1.2.1 Security Categorization Report

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 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 IFF, the electronic transactions (Inquire, Create, Delete, and Modify) and requisite authentication level, and electronic records disposition.

1.2.1.1 Privacy Impact Assessment

The Contractor shall review and propose changes to the NRC completed privacy impact assessments for consistency with Section 208 of the Electronic Government Act, and information obtained during the systems security categorization.

1.2.1.2 Electronic Records Management Disposition

The Contractor shall review and propose changes to the NRC completed electronic records management forms (NRC Form 616 and NRC Form 637) for all NRC IT systems consistent with Code of Federal Regulations Part 36 and OMB Circular A-130, and information obtained during the system's security categorization.

1.2.1.3 E-Authentication Risk Assessments

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.

1.2.2 Risk Assessment

The assessment of risk and the development of system security plans are two important activities in an agency's information security program that directly support security accreditation and are required by the 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 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 risk 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. 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 will track any residual risk in the POAM. 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 POAM.

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

1.2.3 Systems Security Plan (SSP)

The security plan shall be developed in accordance with NIST SP 800-53 Recommended Security Controls for Federal Information Systems, NIST SP 800-37 Guide for the Security Certification and Accreditation of Federal Information Systems, and the NRC IT Security Plan Template. The Contractor shall identify within the SSP the necessary security controls required, citing the security controls that are in place, those that are planned, and those that are not applicable.

Where a system relies upon a control that is provided by another system (e.g. the NRC LAN/WAN), the specific control being relied upon shall be noted along with the name of the system providing that control. The Contractor shall trace the security controls to specific documented guidance, NRC policy (e.g., Management Directives), infrastructure policy or procedures.

The system security plan shall be documented in a report that follows the NRC Template for System Security Plan. The report shall be delivered in draft form and then in pre-system ST&E form after NRC comments are incorporated. The NRC IT Security staff review of the draft is required to ensure compliance. The Contractor shall update the system security plan after completion of the ST&E test report to reflect validated in-place and planned controls. The NRC SITSO must approve the final to enable system accreditation.

1.2.3.1 System Security Controls and Security Requirements Support

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

1.2.4 Review, Verification, and Validation of Security Controls and Requirements

The Contractor shall review, verify, and validate all security controls and security requirements and associated technical resolutions, risk mitigation, and implementations contained within various NRC security and systems development documentation or the Rational Suite Enterprise such that confirmation that the system and associated controls are operating as intended.

1.2.5 Systems Security Controls and Security Requirements Test Plan Development Support

The Contractor shall support the NRC staff in the development and documentation of a test plan within the Rational Suite Enterprise that exercises the systems security controls and security requirements and associated technical resolutions, risk mitigation, and implementations such that confirmation that the system and associated controls are operating as intended and in accordance with NIST SP 800-53 Recommended Security Controls for Federal

Information Systems, NIST SP 800-37 Guide for the Security Certification and Accreditation of Federal Information Systems, and the NRC System Security Test and Evaluation Plan Template. The Contractor shall provide detailed test procedures to ensure all IT security functional and assurance requirements are fully tested. The procedures shall contain sufficient detail that a technically trained individual not familiar with the system can successfully follow the procedures.

The ST&E plan shall identify all testing assumptions, constraints, and dependencies and include a proposed schedule that identifies which personnel, hardware, software, and other requirements that must be met for each portion of the schedule to accomplish full system security testing of all system security functional and assurance requirements where the requirements are not stated as being fulfilled by another system. The following test methods shall be used:

1.2.5.1 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.

1.2.5.2 Demonstration

The Contractor will observe randomly individuals to verify that activities on the system follow the documented procedure or process as the activity is performed. (Example: Observe visitors upon computer room entry in order to verify that all visitation procedures are followed.)

1.2.5.3 Interview

The Contractor will interview personnel to verify the security policies and procedures are understood as implemented and prescribed by governing policies and regulations.

1.2.5.4 Inspection

The Contractor will review and analyze visitor logs to verify all information requested has been entered on the log. (Example: The Contractor shall verify that the visitor's name, signature, organization, reason of visit, arrival and departure date, time, and the escort's name, initials, or signature are included on the log sheets.)

1.2.5.5 Technical Test

The Technical Test verification method shall be used to verify that each implemented control is functioning as intended with the Contractor attempting to access a system by logging on to that system from his workstation (or other device) using an incorrect password to see if the system responds with an error message stating incorrect password or denies access after exceeding the maximum threshold for logon attempts and is directed to call the system administrator to gain access.

Testing requirements that are stated as being fulfilled by another system (provider) shall be accomplished by verifying that the provider system security plan in-place controls meet the requirement.

1.2.6 Review, Verification, and Validation of Security Controls and Requirements Test Plan and Test Plan Execution

The Contractor shall independently review, verify, and validate all systems security test plans and procedures to ensure the accuracy and adequacy of documented test procedures for all systems security controls and security requirements and associated technical resolutions, risk mitigation, and implementations contained within various NRC security and systems development documentation or the Rational Suite Enterprise such that confirmation that the system and associated controls are operating as intended. The Contractor shall update the ST&E Plan after completion of the system security test and evaluation plan test report to reflect validated information. The NRC SITSO must approve the final to enable system accreditation.

1.2.7 Contingency Plan

The Contractor shall support the NRC staff in the development and documentation of a contingency plan and test procedures within the Rational Suite Enterprise. The contingency plan shall be developed in accordance with NIST SP 800-34 Contingency Planning Guide for Information Technology Systems, NIST SP 800-37 Guide for the Security Certification and Accreditation of Federal Information Systems, and the NRC CP Template. The Contractor shall provide detailed procedures for the notification and activation phase, recovery operations, and return to normal operations. The procedures shall contain sufficient detail that a technically trained individual not familiar with the system can successfully follow the procedures. The system contingency plan shall also contain sufficient personnel contact information to enable contact at all times, vendor contact information to enable contact at all times, equipment (hardware and software) and specification information to enable reconstitution of the system from scratch, all service level agreements and memoranda of understanding, the IT standard operating procedures for the system, identification of any systems that this system is dependent upon along with references for the applicable contingency plans, references to the emergency management plan and occupant evacuation plan, and references to the appropriate continuity of operations plan.

The system contingency plan shall be documented in a report that follows the NRC Template for System Contingency Plan. The report shall be delivered in draft form and then in pre-Test form after NRC comments are incorporated. The NRC IT Security staff review of the draft is required to ensure compliance. The Contractor shall update the system contingency plan after completion of the contingency plan test report to reflect validated information. The NRC Senior IT Security Officer must approve the final to enable system accreditation.

1.2.8 Contingency Planning Test and Report

The Contractor shall provide expert advice and support during the Contingency Planning Test to ensure test plan documentation is compliant with the system CP that has been approved by the NRC SITSO. Testing shall follow the test procedures developed and documented by the Contractor within the Rational Suite Enterprise. The Contractor shall document the testing in a System CP Test Report. The CP Test Report shall be developed in accordance with NIST SP 800-34 Contingency Planning Guide for Information Technology Systems, NIST SP 800-37 Guide for the Security Certification and Accreditation of Federal Information Systems, and the NRC Contingency Test Report Template.

The CP Test shall be documented in a report that follows the NRC Template for NRC Contingency Test Report. The CP Test Report shall identify all testing assumptions, constraints, and dependencies as well as any anomalies, impromptu tests, and deviations encountered during testing. The CP Test Report shall include the actual testing schedule and detailed test results for each test procedure outlining specific errors encountered. The CP Test Report shall include a table of test findings incorporating any test issues and recommendations. The CP Test Report shall identify any problems encountered during testing and identify the resulting action items for the system. The CP Test Report shall be delivered in draft form and then in final form after NRC comments are incorporated. The NRC SITSO must approve the final CP Test Report to enable system accreditation.

1.2.9 Quarterly Penetration and Vulnerability Scanning

The Contractor shall perform quarterly analysis, penetration, vulnerability, configuration, systems integrity, and patch management scans. The Contractor shall identify, analyze, and propose tested corrective actions that address POAM items as identified by the SITSO, ensure that controls are operating as intended, and assure the currency of the systems security posture is consistent with the latest DISA and CIS benchmarks and scoring tools available at the time of analysis.

1.2.10 Annual Analysis of Systems Documentation, Security Controls, Requirements, and Implementation Status

The Contractor shall conduct on all "Major Application" and "GSS" NRC systems an inclusive independent audit annually that shall include but is not limited to the review, verification, and validation of all current systems documentation, analysis, penetration, vulnerability, configuration, systems integrity, and patch management scans. The Contractor shall identify, analyze, and propose tested corrective actions that ensure the currency of the systems security posture and ensures that controls are operating as intended. The Contractor shall identify NRC information

systems security vulnerability trends at an agency and system level with special attention to those deficiencies that would impact NRC FISMA compliance.

1.2.11 Development, Update and Maintenance of Common Control Sets and Procedures

The Contractor shall develop a standardized set of streamlined security certification and accreditation documentation that focuses on the functional alignment of common security control sets and standard operating procedures for LOW, MODERATE, and HIGH Baseline systems consistent with FISMA, and NIST SP 800-53 that integrate with the NRC PMM and EA within the Rational Suite Enterprise.

1.2.12 Security Engineering, and Common Security Controls Support

The Contractor shall provide Security Engineering support for application development and information systems solution assessment and proposal such that information systems architectures proposed for implementation at the NRC are based on sound security engineering principles and practices. The contract shall support the NRC EA staff in the development of the security line of business program and documentation, and support the NRC in the assessment, documentation, and implementation of common security solutions OMB information systems security line of business integration.

1.2.13 Security Reporting

In addition to the applicable requirements, the Contractor shall provide a Plan of Action and Milestone Status Tracking Report, FISMA Compliance and Health Report, Risk and Security Vulnerability Trending Report, Security Scoping and Categorization Report, and Security Costs Report.

1.3 LISTED SYSTEM

1.3.1 Security Categorization Report

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 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 IFF, the electronic transactions (Inquire, Create, Delete, and Modify) and requisite authentication level, and electronic records disposition.

1.3.1.1 Privacy Impact Assessment

The Contractor shall review and propose changes to the NRC completed privacy impact assessments for consistency with Section 208 of the Electronic Government Act, and information obtained during the systems security categorization.

1.3.1.2 Electronic Records Management Disposition

The Contractor shall review and propose changes to the NRC completed electronic records management forms (NRC Form 616 and NRC Form 637) for all NRC IT systems consistent with Code of Federal Regulations Part 36 and OMB Circular A-130, and information obtained during the systems security categorization.

1.3.1.3 E-Authentication Risk Assessments

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, NIST SP 800-63 as part of the security categorization.

1.3.2 Risk Assessment

The assessment of risk and the development of system security plans are two important activities in an agency's information security program that directly support security accreditation and are required by the 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 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 risk 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. The NRC IT Security staff review of the draft is required to ensure compliance. The NRC SITSO must approve the final to enable system accreditation.

The Contractor will track any residual risk in the plan of action and milestones POAM. 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 POAM.

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

1.3.3 Systems Security Plan (SSP)

The security plan shall be developed in accordance with NIST SP 800-53 Recommended Security Controls for Federal Information Systems, NIST SP 800-37 Guide for the Security Certification and Accreditation of Federal Information Systems, and the NRC IT Security Plan Template. The Contractor shall identify within the SSP the necessary security controls required, citing the security controls that are in place, those that are planned, and those that are not applicable.

Where a system relies upon a control that is provided by another system (e.g. the NRC LAN/WAN), the specific control being relied upon shall be noted along with the name of the system providing that control. The Contractor shall trace the security controls to specific documented guidance, NRC policy (e.g., Management Directives), infrastructure policy or procedures.

The system security plan shall be documented in a report that follows the NRC Template for System Security Plan. The report shall be delivered in draft form and then in pre-system ST&E form after NRC comments are incorporated. The NRC IT Security staff review of the draft is required to ensure compliance. The Contractor shall update the system security plan after completion of the ST&E test report to reflect validated in-place and planned controls. The NRC SITSO must approve the final to enable system accreditation.

1.3.3.1 System Security Controls and Security Requirements Support

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

1.3.4 Review, Verification, and Validation of Security Controls and Requirements

The Contractor shall review, verify, and validate all security controls and security requirements and associated technical resolutions, risk mitigation, and implementations contained within various NRC security and systems development documentation or the Rational Suite Enterprise such that confirmation that the system and associated controls are operating as intended.

1.4 E-GOVERNMENT SYSTEM

1.4.1 Security Categorization Report

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 SP Series 800. Systems shall be categorized as Major Application, General Support System, or Listed 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 IFF, the electronic transactions (Inquire, Create, Delete, and Modify) and requisite authentication level, and electronic records disposition.

1.4.1.1 Privacy Impact Assessment

The Contractor shall review and propose changes to the NRC completed privacy impact assessments for consistency with Section 208 of the Electronic Government Act, and information obtained during the systems security categorization.

1.4.1.2 Electronic Records Management Disposition

The Contractor shall review and propose changes to the NRC completed electronic records management forms (NRC Form 616 and NRC Form 637) for all NRC IT systems consistent with Code of Federal Regulations Part 36 and OMB Circular A-130, and information obtained during the systems security categorization.

1.4.1.3 E-Authentication Risk Assessments

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.

1.5 OTHER SYSTEM

1.5.1 Security Categorization Report

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 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 IFF, the electronic transactions (Inquire, Create, Delete, and Modify) and requisite authentication level, and electronic records disposition.

1.5.1.1 Privacy Impact Assessment

The Contractor shall review and propose changes to the NRC completed privacy impact assessments for consistency with Section 208 of the Electronic Government Act, and information obtained during the systems security categorization.

1.5.1.2 Electronic Records Management Disposition

The Contractor shall review and propose changes to the NRC completed electronic records management forms (NRC Form 616 and NRC Form 637) for all NRC IT systems consistent with Code of Federal Regulations Part 36 and OMB Circular A-130, and information obtained during the systems security categorization.

1.5.1.3 E-Authentication Risk Assessments

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.

2.0 ISS PROGRAM CLASSIFIED

The Contractor shall support the NRC staff in the development of hard copy certification and accreditation documentation for DAA review and approval of classified NRC information systems consistent with compartmented and trusted information systems security engineering principles, and in compliance with National Security Systems and Intelligence Systems classified/trusted information systems application development, and security certification and accreditation guidance including but not limited to:

- Executive Order 12333;
- Executive Order 12356;
- Executive Order 13356;
- Title 42, United States Code (U.S.C.), 2011 et seq., Atomic Energy Act of 1954;
- Director of Central Intelligence Directive (DCID) 1/7;
- DCID 1/14;
- DCID 1/16;
- DCID 1/19;
- DCID 1/20;
- DCID 1/21;
- DCID 1/22;
- DCID 6/1;
- DCID 6/3;
- DCID 6/5;
- DCID 8-1;
- Homeland Security Presidential Directive 7;
- Homeland Security Presidential Directive 12;
- National Security Directive 42;
- Intelligence Reform and Terrorism Prevention Act;
- Federal Information Processing Standard 199;
- Federal Information Processing Standard 200;
- Federal Information Processing Standard 201;
- NIST 800 Series (Including but not limited to 800-59);

- National Strategy for Secure Cyberspace;
- Other applicable United States Government requirements, guidance, policy, procedures associated with the design, security engineering, development, integration, security certification and accreditation, and deployment of compartmentalized and trusted information systems involved in the processing of classified information.

All classified information provided or generated pursuant to this contract shall be protected as follows:

- The Contractor shall not disclose the classified information to a third party government, person, or firm, or representative thereof, without the prior written consent of the releasing government.
- The Contractor shall provide the classified information a degree of protection no less stringent than that provided by the releasing government in accordance with National Security regulations and as prescribed by its NSA/DSA.
- The Contractor shall not use the classified information for any purpose other than for which it was provided or generated, without the prior written consent of the releasing government.
- All classified information provided or generated pursuant to this contract shall be transferred internationally only through government channels or as specified in writing by the Governments concerned.
- All classified information shall only be disclosed to individuals who have an official need-to-know for the performance of the contract and who have a Personnel Security Clearance at least equal to the classification of the information involved.
- All classified information provided pursuant to this contract shall be marked by the recipient with its government's equivalent security classification.
- All classified information generated pursuant to this contract shall be assigned a security classification in accordance with the security classification specifications.
- All cases in which it is known or there is reason to suspect, that classified information provided or generated pursuant to this contract has been lost or disclosed to unauthorized persons, shall be reported promptly and fully in accordance with National Regulations.
- All classified materials no longer required shall be returned to the originator.
- All classified information provided or generated pursuant to this contract shall not be further provided to another potential Contractor or subcontractor unless:
 - Written assurance is obtained from the recipient's NSA/DSA to the effect that the potential Contractor or subcontractor has been approved for access to CLASSIFIED information by its NSA/DSA; and,
 - Written consent is obtained from the contracting authority for the prime contract if the potential subcontractor is located in a third country.

All classified information and material provided or generated under this contract will continue to be protected in the event of withdrawal by the recipient party or upon termination of the contract, in accordance with national regulations. The Contractor shall comply with all NIACAP and National Security Agency (NSA) guidance for the certification and accreditation of NRC classified systems.

2.1 Security Categorization Report

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 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 IFF, the electronic transactions (Inquire, Create, Delete, and Modify) and requisite authentication level, and electronic records disposition.

2.1.1 Privacy Impact Assessment

The Contractor shall review and propose changes to the NRC completed privacy impact assessments for consistency with Section 208 of the Electronic Government Act, and information obtained during the systems security categorization.

2.1.2 Electronic Records Management Disposition

The Contractor shall review and propose changes to the NRC completed electronic records management forms (NRC Form 616 and NRC Form 637) for all NRC IT systems consistent with Code of Federal Regulations Part 36 and OMB Circular A-130, and information obtained during the systems security categorization.

2.1.3 E-Authentication Risk Assessments

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.

2.2 Risk Assessment

The assessment of risk and the development of system security plans are two important activities in an agency's information security program that directly support security accreditation and are required by the 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 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 risk 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. 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 will track any residual risk in the POAM. 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 POAM.

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

2.3 Systems Security Plan (SSP)

The security plan shall be developed in accordance with NIST SP 800-53 Recommended Security Controls for Federal Information Systems, NIST SP 800-37 Guide for the Security Certification and Accreditation of Federal Information Systems, and the NRC IT Security Plan Template. The Contractor shall identify within the SSP the necessary security controls required, citing the security controls that are in place, those that are planned, and those that are not applicable.

Where a system relies upon a control that is provided by another system (e.g. the NRC LAN/WAN), the specific control being relied upon shall be noted along with the name of the system providing that control. The Contractor shall trace the security controls to specific documented guidance, NRC policy (e.g., Management Directives), infrastructure policy or procedures.

The system security plan shall be documented in a report that follows the NRC Template for System Security Plan. The report shall be delivered in draft form and then in pre-system ST&E form after NRC comments are incorporated. The NRC IT Security staff review of the draft is required to ensure compliance. The Contractor shall update the system security plan after completion of the ST&E test report to reflect validated in-place and planned controls. The NRC SITSO must approve the final to enable system accreditation.

2.4 Contingency Plan

The contingency plan shall be developed in accordance with NIST SP 800-34 Contingency Planning Guide for Information Technology Systems, NIST SP 800-37 Guide for the Security Certification and Accreditation of Federal Information Systems, and the NRC CP Template. The Contractor shall provide detailed procedures for the notification and activation phase, recovery operations, and return to normal operations. The procedures shall contain sufficient detail that a technically trained individual not familiar with the system can successfully follow the procedures. The system contingency plan shall also contain sufficient personnel contact information to enable contact at all times, vendor contact information to enable contact at all times, equipment (hardware and software) and specification information to enable reconstitution of the system from scratch, all service level agreements and memoranda of understanding, the IT standard operating procedures for the system, identification of any systems that this system is dependent upon along with references for the applicable contingency plans, references to the emergency management plan and occupant evacuation plan, and references to the appropriate continuity of operations plan.

The system contingency plan shall be documented in a report that follows the NRC Template for the System CP. The report shall be delivered in draft form and then in pre-test form after NRC comments are incorporated. The NRC IT Security staff review of the draft is required to ensure compliance. The Contractor shall update the system CP after completion of the contingency plan test report to reflect validated information. The NRC SITSO must approve the final to enable system accreditation.

2.5 Contingency Planning Test and Report

The Contractor shall provide expert advice and support during the CP test to ensure test plan documentation is compliant with the system CP that has been approved by the NRC SITSO. Testing shall follow the test procedures documented in the CP. The Contractor shall document the testing in a system CP Test Report. The CP Test Report shall be developed in accordance with NIST SP 800-34 Contingency Planning Guide for Information Technology Systems, NIST SP 800-37 Guide for the Security Certification and Accreditation of Federal Information Systems, and the NRC CP Test Report Template.

The CP Test shall be documented in a report that follows the NRC Template for NRC CP Test Report. The CP Test Report shall identify all testing assumptions, constraints, and dependencies as well as any anomalies, impromptu

tests, and deviations encountered during testing. The CP Test Report shall include the actual testing schedule and detailed test results for each test procedure outlining specific errors encountered. The CP Test Report shall include a table of test findings incorporating any test issues and recommendations. The CP Test Report shall identify any problems encountered during testing and identify the resulting action items for the system. The CP Test Report shall be delivered in draft form and then in final form after NRC comments are incorporated. The NRC SITSO must approve the final CP Test Report to enable system accreditation.

2.6 System Test and Evaluation (ST&E) Plan

The Contractor shall develop a ST&E plan. The system ST&E 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 System Security Test and Evaluation Plan Template. The Contractor shall provide detailed test procedures to ensure all IT security functional and assurance requirements are fully tested. The procedures shall contain sufficient detail that a technically trained individual not familiar with the system can successfully follow the procedures.

The ST&E plan shall identify all testing assumptions, constraints, and dependencies and include a proposed schedule that identifies which personnel, hardware, software, and other requirements that must be met for each portion of the schedule to accomplish full system security testing of all system security functional and assurance requirements where the requirements are not stated as being fulfilled by another system. The following test methods shall be used:

2.6.1 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.

2.6.2 Demonstration

The Contractor will observe randomly individuals to verify that activities on the system follow the documented procedure or process as the activity is performed. (Example: Observe visitors upon computer room entry in order to verify that all visitation procedures are followed.)

2.6.3 Interview

The Contractor will interview personnel to verify the security policies and procedures are understood as implemented and prescribed by governing policies and regulations.

2.6.4 Inspection

The Contractor will review and analyze visitor logs to verify all information requested has been entered on the log. (Example: The Contractor shall verify that the visitor's name, signature, organization, reason of visit, arrival and departure date, time, and the escort's name, initials, or signature are included on the log sheets.)

2.6.5 Technical Test

The Technical Test verification method shall be used to verify that each implemented control is functioning as intended with the Contractor attempting to access a system by logging on to that system from his workstation (or other device) using an incorrect password to see if the system responds with an error message stating incorrect password or denies access after exceeding the maximum threshold for logon attempts and is directed to call the system administrator to gain access.

Testing requirements that are stated as being fulfilled by another system (provider) shall be accomplished by verifying that the provider system security plan in-place controls meet the requirement.

The ST&E plan shall be documented in a report that follows the NRC Template for the System Security Test and Evaluation Plan. The report shall be delivered in draft form and then in pre-Test form after NRC comments are incorporated. The NRC IT Security staff review of the draft is required to ensure compliance. The Contractor shall update the ST&E plan after completion of the system security test and evaluation plan test report to reflect validated information. The NRC Senior IT Security Officer must approve the final to enable system accreditation.

2.7 System Test and Evaluation Report

The Contractor shall support the NRC in the testing validation of the ST&E plan that has been approved and signed by the NRC SITSO. Testing shall follow the approved test procedures documented in the ST&E plan. The Contractor shall document the testing in a ST&E report. The System ST&E report 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 System Security Test and Evaluation Report Template.

The Contractor shall document the results of the ST&E test in a report that follows the NRC Template for the System Security Test and Evaluation Report. The ST&E report shall identify all testing assumptions, constraints, and dependencies as well as any anomalies, impromptu tests, and deviations encountered during testing. The ST&E report shall include the actual testing schedule and detailed test results for each test procedure outlining specific errors encountered. The ST&E report shall include a summary of the system scans and a table of test findings incorporating any test issues and recommendations. The ST&E report shall identify any requirements that have not been met and identify the resulting impact to the system. The ST&E report shall be delivered in draft form and then in final form after NRC comments are incorporated. The NRC SITSO must approve the final ST&E report to enable system accreditation.

LIST OF CONTRACT ATTACHMENTS

- ATTACHMENT A – BASE YEAR DETAILED COSTS/PRICING [REFERENCE SECTION B.1]
(3 PAGES)
- ATTACHMENT B – OPTION YEAR 1 DETAILED COSTS/PRICING [REFERENCE SECTION B.2]
(4 PAGES)
- ATTACHMENT C – OPTION YEAR 2 DETAILED COSTS/PRICING [REFERENCE SECTION B.3]
(4 PAGES)
- ATTACHMENT D – OPTION YEAR 3 DETAILED COSTS/PRICING [REFERENCE SECTION B.4]
(4 PAGES)
- ATTACHMENT E – OPTION YEAR 4 DETAILED COSTS/PRICING [REFERENCE SECTION B.5]
(4 PAGES)
- ATTACHMENT F - LABOR CATEGORY MAPPING (1 PAGE)