

**ORDER FOR SUPPLIES OR SERVICES**

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

1. DATE OF ORDER 09-27-2001		2. CONTRACT NO. (If any) GS-35F-0079J		6. SHIP TO:	
3. ORDER NO. NRC-33-01-191-002		MODIFICATION NO. 002		4. REQUISITION/REFERENCE NO. CI0-01-179-007	
5. ISSUING OFFICE (Address correspondence to) U.S. Nuclear Regulatory Commission Division of Contracts and Property Mgt. Attn: T-7-I-2 IT Acquisition Management Branch Washington DC 20555				a. NAME OF CONSIGNEE U.S. Nuclear Regulatory Commission	
				b. STREET ADDRESS ATTN: Louis Numkin Mail Stop: T-6F15	
				c. CITY Washington	e. ZIP CODE 20555
				d. STATE DC	
7. TO:				f. SHIP VIA	
a. NAME OF CONTRACTOR Allied Technology				8. TYPE OF ORDER	
b. COMPANY NAME ATTN: William P. Conner 1803 Research Boulevard				<input type="checkbox"/> a. PURCHASE ORDER	
c. STREET ADDRESS Suite 601				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				<input checked="" type="checkbox"/> b. DELIVERY/TASK ORDER	
e. STATE MD				Except for billing instructions on the reverse, this delivery/task order is subject to instructions contained on this side only of this form and is issued subject to the terms and conditions of the above-numbered contract.	
f. ZIP CODE 20850					
9. ACCOUNTING AND APPROPRIATION DATA 31X0200.110 JCN: J2923 B&R: 12015101160 BOC: 252A OBLIGATE: \$130,419.20				10. REQUISITIONING OFFICE cio OCIO/PRMD	

11. BUSINESS CLASSIFICATION (Check appropriate box(es))			
<input checked="" type="checkbox"/> a. SMALL	<input type="checkbox"/> b. OTHER THAN SMALL	<input checked="" type="checkbox"/> c. DISADVANTAGED	<input type="checkbox"/> d. WOMEN-OWNED
12. F.O.B. POINT Destination		14. GOVERNMENT B/L NO.	15. DELIVER TO F.O.B. POINT ON OR BEFORE See Below
13. PLACE OF		16. DISCOUNT TERMS N/A	
a. INSPECTION		b. ACCEPTANCE	
17. SCHEDULE (See reverse for Rejections) See CONTINUATION Page			

ITEM NO. (A)	SUPPLIES OR SERVICES (B)	QUANTITY ORDERED (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)	QUANTITY ACCEPTED (G)
	The U.S. Nuclear Regulatory Commission (NRC) hereby accepts Allied's proposal dated 9/19/01, which is hereby incorporated by reference and made a part of this order. The labor categories for Deliverables 1,2,3, & 5 are as follows: 1 Senior Management Analyst/Project Manager - 16 hours 1 Senior Management Analyst - 134 hours Senior Information Engineer	150	Hours	117.28	\$17,592.00	
	Senior Computer Systems Analyst	670	Hours	92.85	\$62,209.50	
	Inidirect costs The labor categories for Deliverable Item 4 (Optional) Senior Management Analyst/PM 6 hrs \$117.28 \$703.68 Senior Management Analyst 62 hrs \$117.28 \$7,271.36 Senior Info. Engineer 328 hrs \$92.85 \$30,454.80 Sr. Computer Systems Analyst 328 hrs \$73.31 \$24,045.68 Total Fixed Price Ceiling of Optional Task \$62,975.52	670	Hours	73.31	\$49,117.70	
	The fixed price of this delivery order is \$130,419.20 for deliverables 1,2,3, and 5.	1	each	1,500.00	\$1,500.00	

18. SHIPPING POINT		19. GROSS SHIPPING WEIGHT		20. INVOICE NO.		\$130,419.20	<b>SUBTOTAL</b>	
21. MAIL INVOICE TO:								
SEE BILLING INSTRUCTIONS ON REVERSE		a. NAME U.S. Nuclear Regulatory Commission Division of Contracts & Property Mgmt.						17(h) <b>TOTAL</b> (Cont. pages)
		b. STREET ADDRESS (or P.O. Box) ATTN: Mail Stop T-7-I2						17(i). <b>GRAND TOTAL</b>
		c. CITY Washington	d. STATE DC	e. ZIP CODE 20555				\$130,419.20
22. UNITED STATES OF AMERICA BY (Signature) 				23. NAME (Typed) Mark J. Flynn Contracting Officer TITLE: CONTRACTING/ORDERING OFFICER				

**ORDER FOR SUPPLIES OR SERVICES  
SCHEDULE - CONTINUATION**

PAGE NO  
2

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

DATE OF ORDER 09-27-2001	CONTRACT NO. GS-35F-0079J	ORDER NO. NRC-33-01-191-002
-----------------------------	------------------------------	--------------------------------

ITEM NO. (A)	SUPPLIES OR SERVICES (B)	QUANTITY ORDERED (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)	QUANTITY ACCEPTED (G)
-----------------	-----------------------------	----------------------------	-------------	----------------------	---------------	-----------------------------

The ceiling of Optioal task (Deliverable 4) is \$62,975.52.  
The Optional task can only be exercised by the Contracting  
Officer through written modification to this order.

The amount obligated under this order is \$130,419.20. Any  
amount undertaken by the Contractor in excess of the  
obligated amount specified above is done so at the  
Contractor's sole risk.

FAR Clause 52.232-7 is applicable to this order.

The period of performance forthe based period is estimated  
to be 8 months from date of award. The option period is  
anticipated to be 4 months if exercised under this delivery  
order.

The project officer is Lou Numkin (301) 415-5906.

Attachments:  
Statement of Work  
  
Billing Instructions  
ACH Vendor Information Form

TOTAL CARRIED FORWARD TO 1ST PAGE (ITEM 17(H))



## TASK ORDER TERMS AND CONDITIONS

NOT SPECIFIED IN THE CONTRACT

### A.1 NRC ACQUISITION CLAUSES - (NRCAR) 48 CFR CH. 20

2052.209-72

CONTRACTOR ORGANIZATIONAL CONFLICTS OF INTEREST JAN 1993

### A.2 ELECTRONIC PAYMENT

The Debt Collection Improvement Act of 1996 requires that all payments except IRS tax refunds be made by Electronic Funds Transfer. It is the policy of the Nuclear Regulatory Commission to pay vendors by the Automated Clearing House (ACH) electronic funds transfer payment system. The electronic system is known as Vendor Express. Payment shall be made in accordance with FAR 52.232-33, entitled "Mandatory Information for Electronic Funds Transfer Payment".

To receive payment, the contractor shall complete the "Company Information" portion of the Standard Form 3881, entitled "ACH Vendor/Miscellaneous Payment Enrollment Form" found as an attachment to this document. The contractor shall take the form to the ACH Coordinator at the financial institution that maintains its company's bank account. The contractor shall discuss with the ACH Coordinator how the payment identification information (addendum record) will be passed to them once the payment is received by the financial institution. Further information concerning the addendum is provided at Attachment . The ACN Coordinator should fill out the "Financial Institution Information" portion of the form and return it to the Office of the Controller at the following address: Nuclear Regulatory Commission, Division of Accounting and Finance, Financial Operations Section, Mail Stop T-9-H-4, Washington, DC 20555, ATTN: ACH/Vendor Express. It is the responsibility of the contractor to ensure that the financial institution returns the completed form to the above cited NRC address. If the contractor can provide the financial information, signature of the financial institutions ACH Coordinator is not required. The NRC is under no obligation to send reminders. Only after the Office of the Controller has processed the contractor's sign-up form will the contractor be eligible to receive payments.

Once electronic funds transfer is established for payments authorized by NRC, the contractor needs to submit an additional SF 3881 only to report changes to the information supplied.

Questions concerning ACH/Vendor Express should be directed to the Financial Operations staff at (301) 415-7520."

### A.3 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.

Technical Requirements for Contractor to  
Provide Computer Security Services to the  
NRC Office of Nuclear Reactor Regulation (NRR)

## **1.0 BACKGROUND**

The Contractor shall submit a firm-fixed price (FFP) proposal in response to a request to provide computer security services to the U.S. Nuclear Regulatory Commission (NRC), Office of Nuclear Reactor Regulation (NRR).

The mission of the NRC is to ensure adequate protection for the public health and safety, promote the common defense and security, and protect the environment in regulating the Nation's civilian uses of nuclear fuels and material. In this undertaking, the NRC oversees nuclear power plants, non-power reactors, nuclear fuel cycle facilities, waste disposal, and the industrial and medical uses of nuclear materials. NRC works closely with its licensees and with local, state, other Federal and international organizations to achieve its goals in the event of an emergency. NRR is the office which is responsible for oversight of nuclear power plants and non-power reactors.

The Office of Chief Information Officer (OCIO) is responsible for guiding the NRC in the effective and efficient use and integration of appropriate information technologies to accomplish the NRC mission. A portion of those responsibilities involves computer security administration, handled by the OCIO Computer Security Staff.

In accordance with the Office of Management and Budget (OMB) Circular A-130, Appendix III, the NRC is required to perform risk assessments, develop system security plans, develop security test plans, test security features, develop security test reports, prepare business continuity plans, and prepare a certification report for its sensitive systems.

The NRC requires the support of a Contractor to develop the appropriate security documentation for two (2) NRR sensitive systems (i.e., the Reactor Program System (RPS), the Allegation Management System (AMS)), and one optional sensitive system - the Operator Licensing Tracking System (OLTS), to ensure compliance with current Federal guidelines. Each of the three (3) systems require that the following items be developed: a Risk Assessment Report, a System Security Plan (SSP), a Security Test & Evaluation (ST&E) Test Plan and Report, a Business Continuity Plan (BCP), and a System Certification Report.

### **1.1 SYSTEM DESCRIPTIONS**

#### **1.1.1 Reactor Program System (RPS)**

The RPS was initiated in 1995, when NRR recognized the need to gain regulatory and administrative improvements and efficiencies. NRR initiated the program with Information Resources Management Office (IRM) and the regions to integrate about 11 mainframe systems, serving the reactor program in Headquarters (HQ) and the regions, into one (1) integrated system using modern client server technology supported by IRM. Many of these older systems did not effectively interface or share information resulting in inefficiencies that impede effective program management.

The RPS provides an integrated methodology for planning, scheduling, conducting, reporting and analyzing most of the functions performed by the approximately 1,300 people involved with

NRR programs in HQ and the regions. The RPS was designed from a geographically indifferent perspective with a uniform user interface focused on the job to be done. A basic premise of the system is that there is central maintenance of common files, with a single point of data entry and sharing of information so that data can be entered once and used throughout any process where needed. Where possible, inherent data quality design was installed up-front to preclude the entry of invalid or inaccurate information and the resulting problems and inefficiencies. RPS and its associated components were designed using client server technology and commercial-off-the-shelf (COTS) products, including PowerBuilder and Sybase. The RPS system design team met with other office representatives in the Office Nuclear Materials Safety and Safeguards (NMSS) and the Office of the Controller (OC) to share design information and ensure that data required by their offices was included in RPS.

The ten (10) modules of the RPS are:

1. Inspection Planning (IP) module
2. Inspection Report Tracking System (IRTS) module
3. Inspection Procedure Authority System (IPAS) module
4. Inspection Planning Cycle (IPC) module
5. Item Reporting (IR) module
6. Licensing and Other Planning (LOP) module
7. Performance Measures (PM) module
8. Security Access Method (SAM) module
9. Safety Issues Management Systems (SIMS) Reports
10. Reactor Oversight Process (ROP)

The RPS collects information once, at the source, and integrates information for both inspections and licensing in one (1) location that can be correlated and analyzed against facility characteristics. The RPS provides an analytical capability that permits the linking, trending and analysis of plant performance information on an on-going basis, so that plant performance characteristics can be better monitored. This includes automating relationships and searches so that inspection findings, event follow-up, cause codes can be correlated with facility characteristics and other program information to more effectively compare plant performance with the norm, and to better identify early causes for concern.

The RPS effort combines technology readily available off-the-shelf with significant changes in the evaluation and information reporting process. The RPS provides for the effective and efficient integration and analysis of information associated with NRR programs conducted in HQ and regions. The information associated with NRR programs includes inspection, licensing, plant performance assessment, events and emergency issues tracking, safety issues management, allegations management and other regulatory activities. RPS provides the necessary information management for the effective and efficient planning, scheduling, resource allocation, reporting and analysis of these programs.

RPS captures data once at the source and eliminates the need to reenter the same data in multiple systems, thereby reducing the data entry requirements as well as the errors and inconsistencies created by multiple entry of the same data in different systems. It creates program efficiencies by maximizing the sharing of information among licensing, inspection, allegations management, events tracking and other reactor oversight programs, and improves program management through functionality which is geographically indifferent. It reduces the current burden of staff and management to compile, review and analyze information that is needed to evaluate the effectiveness of regulatory programs and the information needed to evaluate plant performance. It provides access to data from sites and Regional offices, as well as HQ, so that data is accessible and reportable, and provides the ability to easily analyze regulatory and administrative information for all aspects of the NRR program. The client server database provides enhanced assessment of inspection information through improved word search capability and correlation of findings with facility and program information thereby enabling identification of relationships, trends, and comparative assessments.

### **1.1.2 Allegation Management System (AMS)**

The Allegation Management System (AMS) is used to track allegations concerning activities and facilities within the jurisdiction of the NRC. The client server version of AMS was deployed for use on October 1, 1997, so that individual offices of the NRC could manage information regarding allegations related to NRC regulated facilities more effectively. AMS was designed to assist in the timely collection, storage, and retrieval of key information on Allegations received by the NRC related to NRC regulated facilities. AMS is an online computer application that tracks allegations from receipt to resolution, tracks involvement of regions and program offices, provides basic descriptive and status information, and provides reference to the closeout documentation. The AMS information is stored on a client/server machine so that both Headquarters' and regional users may access and manipulate allegation data as necessary. Only coordinators can add new data, delete or change exiting data, and report on various combinations of data. Other users may be granted view only capabilities.

The file contains data on each allegation as the information is entered using the Allegation, Concern, Action, Facilities, and Outside Organization windows. Queries may be performed and ad hoc reports generated using MS Access software.

### **1.1.3 Operator Licensing Tracking System (OLTS) (OPTIONAL)**

The Operator Licensing Tracking System (OLTS) was developed by the NRC in the early 1980s and converted to its present structure, a client-server application OLTS-R in 2000. The NRR, Division of Inspection Program Management (DIPM), Operator Licensing, Human Performance and Plant Support Branch (IOLB) exercises responsibility for the system. OLTS is categorized as a major application and is in the operational stage of its life cycle

The OLTS application was developed to aid the Headquarters and Regional Operator Licensing Assistants in tracking the logging of applications and operator licenses and in preparing statistical reports. This system maintains a record of all applications received for new operator licenses for all power and non-power reactors, as well as for renewal license applications. Approximately 5,000 active licenses are currently maintained in the system. The reporting function provides the users with a quick reference to the licenses issued at various plants and recorded data concerning the applicants. The data is available for display on an on-line terminal or via hard-copy printer.

## 1.2 SYSTEM ENVIRONMENTS

### 1.2.1 Reactor Program System (RPS)

The RPS was designed to fit within the Agency's client server and local area network (LAN) infrastructure and be accessible via Agency-standard personal computer (PC) workstations (Pentium, running on Windows NT) using COTS software for greater flexibility and ease of maintenance. The system will provide for inherent staff efficiencies and improve data quality through several means which include: the single entry of information for each data element and sharing of the information across all RPS components in an integrated database environment, the central maintenance of common files and tables, and inherent data quality design to include up-front validation of data upon entry and reduction of manual entries where possible.

RPS components reside on the NRC client-server infrastructure (currently RS/6000s) installed in each region and HQ. Data replication is used to maintain data integrity across the network of RS/6000's. All RPS components access a Sybase database with common tables. The COTS capabilities of PowerBuilder have been used for development and access to the data.

Each RPS user requires access to an Agency-standard PC with a minimum of 16MB RAM and 200MB free disk space. The PC Refresh program provided this capacity to all NRC employees, so no extra cost was needed for implementing the RPS project. Each of the sites use the 28.8 baud modem which was installed by IRM as part of the infrastructure upgrade. The sites dial-in to a Cubix box that contains the RPS software. The implementation strategy eliminated the need to install the RPS software at each site. In late 1997, the memory in the Cubix boxes was increased to 132MB, and OCIO and NRR upgraded the memory in each Cubix box processor to 32MB.

The RPS database was implemented using Sybase software and is located on a file server within HQ offices, as well as the Region offices. The database is accessed via a modem, as in the case of Regional Resident Inspectors and via direct connectivity for individuals in HQ or the Regional offices.

### 1.2.2 Allegation Management System (AMS)

The AMS information is a client server application using Sybase and PowerBuilder so that both Headquarters' and regional users may access and manipulate allegation data as necessary. The AMS was designed to fit within the Agency's client server and local area network (LAN) infrastructure and be accessible via Agency-standard personal computer (PC) workstations (*i.e.*, Pentium, running on Windows NT) using COTS software for greater flexibility and ease of maintenance.

AMS components reside on the NRC client-server infrastructure (currently RS/6000s) installed in HQ. All AMS components access a Sybase database with common tables. The COTS capabilities of PowerBuilder have been used for development and access to the data. Each AMS user requires access to an Agency-standard PC with a minimum of 32MB RAM and 200MB free disk space.

The AMS database was implemented using Sybase software and is located on a file server within HQ offices. The database is accessed via direct connectivity for individuals in HQ or the Regional offices.

### **1.2.3 Operator Licensing Tracking System (OLTS) (OPTIONAL)**

The OLTS system was designed to fit within the Agency's client-server and local area network (LAN) infrastructure and be accessible via Agency- standard personal computer (PC) workstations (*i.e.*, Pentium, running on Windows NT). The system provides for inherent staff efficiencies and improves data quality through several means, which include: the single entry of information for each data element and the sharing of information with other databases, *i.e.*, Reactor Program System; inherent data quality design to include validation of data upon entry and the reduction of manual entries, where possible.

OLTS resides on the NRC client-server infrastructure (currently RS/6000s) installed in Headquarters with less than 15 authorized users (two for HQ and *two* for each region with an alternate at each site as well as the appropriate branch chiefs). OLTS users located at regional offices are granted access to all data, but only have update authority to data pertaining to their region. All users have been granted identical functional privileges.

Each RPS user requires access to an Agency-standard PC with a minimum of 16MB RAM and 200MB free disk space. The PC Refresh program provided this capacity to all NRC employees, so no extra cost was needed for implementing the OLTS program.

The OLTS database was implemented using Sybase software and is located on a file server within the NRC Headquarters office. The database is accessed via direct connectivity for individuals in Headquarters or the Regional offices.

## **1.3 SYSTEM INFORMATION SENSITIVITY AND CRITICALITY**

### **1.3.1 Reactor Program System (RPS)**

**Confidentiality:** Roughly 98 percent of the information processed by RPS is publicly available. RPS data that must be safeguarded from disclosure relates to unannounced inspections, draft inspection reports, and one (1) table which contains social security numbers of employees. Inspection files must be kept confidential to prevent disclosure of dates and locations of unannounced inspections. Once the inspections are conducted however, the information is public knowledge. Draft inspection reports are pre-decisional and as such must not be disclosed until approved. Once approved, these reports are open to the public. The social security number table in RPS should not be accessible to those not having a need-to-know. However, it should be noted that this table consists of social security numbers with cross referenced data that would indicate the identity of the person associated with the number. Based on the conclusions reached by the participants, the confidentiality impacts to the system are considered to be only a minor concern. The necessity for maintaining the confidentiality of RPS data is considered to be a minimal security concern, therefore protective requirements are rated as **Low**.

**Integrity:** The data contained in the RPS application is used to manage NRR licensing, inspection, and regulatory programs at NRC HQ and the regions. Should the integrity of RPS data be compromised, NRC could experience operational impacts through inefficient management of its resources, embarrassment due to loss of visibility of program performance indicators, and potential fraud, waste, and abuse. The necessity for maintaining the integrity of RPS data is considered to be an important security concern, therefore protective requirements are rated as **Medium**.

**Availability:** If RPS information were unavailable, the NRC would experience an adverse impact within seven (7) business days. It should be noted that all RPS data is automatically replicated to each of the RS/6000 application servers located in the Regional offices providing an extremely high degree of reliability. An outage of more than seven (7) days would result in the inability to manage and track NRR programs and resources, causing potential embarrassment to the NRC, and would affect public relations with NRR customers. Additionally, the costs associated with loss of productivity and of recreating any lost data would have a significant, but not critical, impact on the NRC budget. The necessity for assuring the availability of RPS data is considered to be an important security concern, therefore protective requirements are rated as **Medium**.

### 1.3.2 Allegation Management System (AMS)

**Confidentiality:** The data in AMS is not normally disclosed. However, some information may be released in response to a request under the Freedom of Information Act. If the information in AMS were inappropriately released, it could result in disclosing the identity of the alleged, which has the potential of exposing the alleged to retaliatory actions. However, using the NIST GISRA criteria, AMS categorizes as **Low** for this element. There are no direct financial consequences for the NRC if the data is released. The agency could be publicly embarrassed by the release and there could be some cost associated with corrective actions.

**Integrity:** The data contained in the AMS application is used to manage followup on allegations and track staff actions. The NRC has several performance measures that are based on data in AMS. The data is also used to identify trends in the industry and at specific licensee facilities. Should the integrity of AMS data be compromised, it would effect the efficiency with which the allegation process conducted, i.e. more resources would be spent manually tracking completion of staff actions. Additionally, the staff would not be able to perform the trending currently performed. However, using the NIST GISRA criteria, AMS categorizes as **Low** for this element.

**Availability:** If AMS information were unavailable, it would effect the efficiency with which the allegation process conducted, i.e. more resources would be spent manually tracking completion of staff actions. Additionally, the staff would not be able to perform the trending currently performed. However, using the NIST GISRA criteria, AMS categorizes as **Low** for this element.

### 1.3.3 Operator Licensing Tracking System (OLTS) (OPTIONAL)

**Confidentiality:** OLTS stores some Privacy Act data in the Sybase tables, in the form of examination information pertaining to operators. This data requires protection from unauthorized disclosure. It was determined from personal interviews and through a review of the data dictionary that the protection requirement for ensuring the confidentiality of OLTS is **High**.

**Integrity:** OLTS stores and processes personal information pertaining to individual operator licensing for certification purposes (e.g., examination scores, medical records and operator licensing data). It is essential that the information be as accurate as possible to accomplish the agency's mission. Therefore, the protection requirement for ensuring the integrity of the OLTS application is **High**.

**Availability:** The Certification Team ascertained from personal interviews that NRC could continue to operate without the OLTS application for one week before a measurable impact on licensing operations would occur. Therefore, the protection requirement for ensuring the availability of the OLTS application is **Low**.

## **2.0 PROPOSAL SOLUTION**

### **2.1 PLANS FOR PERFORMANCE**

The Contractor shall propose to complete this project in five (5) milestones and corresponding deliverables, on a firm-fixed price (FFP) arrangement. Each milestone consists of performing required tasks, as specified in this Statement of Work (SOW), resulting in specific deliverables, as described below:

**Milestone 1:** Project Management Plan

**Milestone 2:** Reactor Program System (RPS)

- ▶ Develop a Risk Assessment Report
- ▶ Develop a System Security Plan
- ▶ Develop a Security Test & Evaluation (ST&E) Plan and Report
- ▶ Develop a Business Continuity Plan
- ▶ Develop a System Certification Report

**Milestone 3:** Allegation Management System (AMS)

- ▶ Develop a Risk Assessment Report
- ▶ Develop a System Security Plan
- ▶ Develop a Security Test & Evaluation (ST&E) Plan and Report
- ▶ Develop a Business Continuity Plan
- ▶ Develop a System Certification Report

#### **Milestone 4: Operator Licensing Tracking System (OLTS) (OPTIONAL)**

- Develop a Risk Assessment Report
- ▶ Develop a System Security Plan
- ▶ Develop a Security Test & Evaluation (ST&E) Plan and Report
- ▶ Develop a Business Continuity Plan
- ▶ Develop a System Certification Report

#### **Milestone 5: Exit Briefing Presentation**

The Contractor shall perform all necessary support activities in a phased approach to ensure the NRC an economy of scale in level of effort and cost-savings. The Contractor shall ensure that specifics pertaining to the system(s) are fully addressed and that the final deliverables can “stand alone” serving as independent documents required for systems certification.

## **2.2 TECHNICAL APPROACH**

### **2.2.1 Milestone 1: Project Management Plan**

The Contractor shall develop a *Project Management Plan* that details project milestones, deliverables, schedules, and management processes. The Contractor shall review published documentation on security plan development; such as National Institute of Standards and Technology (NIST) Special Publication (SP) 800-18, *Guide for Developing Security Plans for Information Technology Systems*; Federal Information Processing Standards Publication (FIPS PUB) 102, *Guidelines for Computer Security Certification and Accreditation*; the Department of Commerce (DOC) *Abbreviated Certification Methodology Guidelines for Sensitive Information Technology Systems*; the Computer Security Act of 1987; OMB Circular A-130, *Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Systems*; Federal statutes and regulations; and NRC management directives. Based on this review, the Contractor shall formulate issues and questions necessary for interview sessions.

The Contractor shall develop a Draft and Final *Project Management Plan* for the NRC NRR task.

### **2.2.2 Milestone 2: Reactor Program System (RPS)**

The Contractor shall perform data collection, interviews, and documentation review and analysis in accordance with the *Project Work Plan* prepared and approved in Milestone 1. Approximately five (5) to ten (10) detailed interviews are anticipated with NRC employees and Contractor personnel located in Rockville, MD. This milestone is divided into four (4) subtasks, with the possibility of adding one (1) additional subtask at a later date.

### **2.2.2.1 Milestone 2-1: Develop a Risk Assessment Report for the RPS**

The Contractor shall coordinate with OCIO management to schedule potential interviews with identified key Agency personnel familiar with the management, operations, and security of the system. The Contractor shall utilize this information to assess the current operating environment, concentrating on analysis of data sensitivity, and identification of threats and vulnerabilities to the NRC RPS system. Based on the results and analysis of interviews and data collection efforts, the Contractor shall conduct a risk assessment of the NRC RPS operating environment, and develop a *Risk Assessment Report* for the NRC RPS.

The objectives of this risk assessment for the NRC RPS shall be to:

- Identify potential undesirable or unauthorized events;
- Identify risks that could have a negative impact on the confidentiality, integrity, or availability of information processed or stored by, or transmitted through the system;
- Identify potential controls to reduce or eliminate the impact of risk events; and
- Establish responsibilities and milestones for the implementation of mitigating controls.

The Contractor shall document the results of this process. This shall include documenting the risk number; a description of each risk; the type of risk (i.e., impacting the confidentiality, integrity, or availability of an asset); the level of concern (i.e., major or minor); the associated controls; and the action(s) required to minimize each risk.

The Contractor shall develop a Draft and Final *Risk Assessment Report* for the NRC RPS.

### **2.2.2.2 Milestone 2-2: Develop the System Security Plan for the RPS**

Based on the results and analysis of interviews and data collection efforts, the Contractor shall develop the *System Security Plan* for the NRC RPS. This plan shall follow the format of NIST SP 800-18, that shall be used as a foundation for the analysis and presentation of essential security plan information. Plan development shall also include a preliminary estimation of the status of necessary safeguards (i.e., in-place, planned, in-place and planned, or not applicable).

As necessary, the Contractor shall develop a set of application Rules of Behavior for inclusion in the *System Security Plan* to ensure compliance with NIST SP 800-18.

The Contractor shall develop the Draft and Final *System Security Plan* for the NRC RPS.

### **2.2.2.3 Milestone 2-3: Develop the Security Test & Evaluation (ST&E) Test Plan and Report for the RPS**

The Contractor shall develop a *Security Test & Evaluation (ST&E) Test Plan* for the RPS in accordance with the *Project Management Plan* prepared and approved in Milestone 1. Additionally, the Contractor shall perform security testing conducted with NRC personnel and shall prepare a *Security Test & Evaluation (ST&E) Test Report* for the NRC RPS. This milestone is divided into two (2) subtasks.

### **Milestone 2-3-1: Develop the Security Test & Evaluation (ST&E) Test Plan**

The Contractor shall develop a test plan for reviewing and testing the security control measures protecting the NRC RPS using the DOC Abbreviated Certification Methodology. The deliverable shall include plans for testing the adequacy of system security safeguards.

The Contractor shall develop a *System Test & Evaluation (ST&E) Test Plan* for the NRC RPS.

### **Milestone 2-3-2: Develop the Security Test & Evaluation (ST&E) Test Report**

The Contractor shall conduct system testing of safeguards for the NRC RPS and provide recommendations for improvements to the system using the *System Security Plan* developed in Milestone 2-2 and the *System Test & Evaluation (ST&E) Test Plan* developed in Milestone 2-3-1. Recommendations for improvements to the NRC RPS shall be made upon evaluation of the system test results, and shall be incorporated into a *Security Test & Evaluation (ST&E) Test Report*. Each safeguard shall be categorized as follows:

**High Priority:** Corrective action should be taken prior to formal certification of the system. Expedient implementation of *High Priority* recommendations is based on the criticality of the affected safeguards to the security of the system. A plan of action for mitigating the situation and implementing corrective actions should be developed and approved by NRC management within thirty (30) days of receipt of the report.

**Moderate Priority:** Though important to enhancing the security of the system, corrective action of *Moderate Priority* risks should be taken irrespective of formal system certification. Where practical and cost effective, these recommendations should be implemented within six (6) months.

**Low Priority:** Corrective action should be taken as soon as practical and cost effective. These recommendations concern actions where the implementation needs to be reviewed to determine if they are practical or cost effective or are beyond the direct control of the system owner and require implementation action by other NRC offices or external agencies. Certification of the system should not be delayed pending resolution of *Low Priority* actions. Nevertheless, they should be closely monitored to ensure that they are implemented as soon as practical and cost effective.

Upon request, approximately two (2) hours of assistance shall be provided to the NRC RPS System Owner to discuss the *Security Test & Evaluation (ST&E) Test Report* to correct deficiencies identified in the testing process.

The Contractor shall develop a *System Test & Evaluation (ST&E) Test Report* for the NRC RPS.

### **2.2.2.4 Milestone 2-4: Develop a Business Continuity Plan for the RPS**

The Contractor shall develop a *Business Continuity Plan* for the NRC RPS in accordance with the *Project Management Plan* prepared and approved in Milestone 1. The plan shall detail procedures for NRC to respond to and recover from operational disasters and shall identify components necessary to provide the support required to continue operations in the event of a disaster. The Contractor shall review system documentation and interview cognizant NRC personnel to identify tasks required to resume emergency-level and full operations related to the NRC RPS; shall determine requirements for restoration of the system to include personnel, hardware, software, media, supplies, facilities, communications, and transportation; shall identify

sources for meeting requirements; and shall document recovery strategies. The Contractor shall provide Living Disaster Recovery Planning System (LDRPS) certified personnel to document the RPS business continuity information within the NRC's LDRPS application.

The Contractor shall develop a Draft and Final *Business Continuity Plan* for the NRC RPS.

#### **2.2.2.5 Milestone 2-5: Develop the System Certification Report for the RPS**

The Contractor shall develop a *System Certification Report* for the NRC RPS in accordance with the *Project Management Plan* prepared and approved in Milestone 1 that shall summarize the results of each step of this milestone. Preparation of certification statements, all worksheets, and documentation required by FIPS Publication 102 shall be submitted for the certification of the NRC RPS.

The *System Certification Report* for the NRC RPS shall include the Risk Assessment Report, System Security Plan, Certification Letter, and Worksheets 1 through 6 from the DOC Abbreviated Certification Methodology. It shall contain recommendations for improvements and recommendations to the accrediting official. The *System Certification Report* shall be prepared in accordance with the Computer Security Act of 1987, Federal statutes and regulations, as well as NRC Management Directive.

The Contractor shall develop the *System Certification Report* for the NRC RPS.

#### **2.2.3 Milestone 3: Allegation Management System (AMS)**

The Contractor shall perform data collection, interviews, and documentation review and analysis in accordance with the *Project Work Plan* prepared and approved in Milestone 1. Approximately five (5) to ten (10) detailed interviews are anticipated with NRC employees and Contractor personnel located in Rockville, MD. This milestone is divided into four (4) subtasks, with the possibility of adding one (1) additional subtask at a later date.

##### **2.2.3.1 Milestone 3-1: Develop a Risk Assessment Report for the AMS**

The Contractor shall coordinate with OCIO management to schedule potential interviews with identified key Agency personnel familiar with the management, operations, and security of the system. The Contractor shall utilize this information to assess the current operating environment, concentrating on analysis of data sensitivity, and identification of threats and vulnerabilities to the NRC AMS system. Based on the results and analysis of interviews and data collection efforts, the Contractor shall conduct a risk assessment of the NRC AMS operating environment, and develop a *Risk Assessment Report* for the NRC AMS.

The objectives of this risk assessment for the NRC AMS shall be to:

- Identify potential undesirable or unauthorized events;
- Identify risks that could have a negative impact on the confidentiality, integrity, or availability of information processed or stored by, or transmitted through the system;
- Identify potential controls to reduce or eliminate the impact of risk events; and
- Establish responsibilities and milestones for the implementation of mitigating controls.

The Contractor shall document the results of this process. This shall include documenting the risk number; a description of each risk; the type of risk (i.e., impacting the confidentiality, integrity, or availability of an asset); the level of concern (i.e., major or minor); the associated controls; and the action(s) required to minimize each risk.

The Contractor shall develop a Draft and Final *Risk Assessment Report* for the NRC AMS.

### **2.2.3.2 Milestone 3-2: Develop the System Security Plan for the AMS**

Based on the results and analysis of interviews and data collection efforts, the Contractor shall develop the *System Security Plan* for the NRC AMS. This plan shall follow the format of NIST SP 800-18, that shall be used as a foundation for the analysis and presentation of essential security plan information. Plan development shall also include a preliminary estimation of the status of necessary safeguards (i.e., in-place, planned, in-place and planned, or not applicable). As necessary, the Contractor shall develop a set of application Rules of Behavior for inclusion in the *System Security Plan* to ensure compliance with NIST SP 800-18.

The Contractor shall develop the Draft and Final *System Security Plan* for the NRC AMS.

### **2.2.3.3 Milestone 3-3: Develop the Security Test & Evaluation (ST&E) Test Plan and Report for the AMS**

The Contractor shall develop a *Security Test & Evaluation (ST&E) Test Plan* for the AMS in accordance with the *Project Management Plan* prepared and approved in Milestone 1. Additionally, the Contractor shall perform security testing conducted with NRC personnel and shall prepare a *Security Test & Evaluation (ST&E) Test Report* for the NRC AMS. This milestone is divided into two (2) subtasks.

#### **Milestone 3-3-1: Develop the Security Test & Evaluation (ST&E) Test Plan**

The Contractor shall develop a test plan for reviewing and testing the security control measures protecting the NRC AMS using the DOC Abbreviated Certification Methodology. The deliverable shall include plans for testing the adequacy of system security safeguards.

The Contractor shall develop a *System Test & Evaluation (ST&E) Test Plan* for the NRC AMS.

#### **Milestone 3-3-2: Develop the Security Test & Evaluation (ST&E) Test Report**

The Contractor shall conduct system testing of safeguards for the NRC AMS and provide recommendations for improvements to the system using the *System Security Plan* developed in Milestone 2-3 and the *System Test & Evaluation (ST&E) Test Plan* developed in Milestone 3-3-1. Recommendations for improvements to the NRC AMS shall be made upon evaluation of the system test results, and shall be incorporated into a *Security Test & Evaluation (ST&E) Test Report*. Each safeguard shall be categorized as follows:

**High Priority:** Corrective action should be taken prior to formal certification of the system. Expedient implementation of *High Priority* recommendations is based on the criticality of the affected safeguards to the security of the system. A plan of action for mitigating the situation and implementing corrective actions should be developed and approved by NRC management within thirty (30) days of receipt of the report.

**Moderate Priority:** Though important to enhancing the security of the system, corrective action of *Moderate Priority* risks should be taken irrespective of formal system certification. Where

practical and cost effective, these recommendations should be implemented within six (6) months.

**Low Priority:** Corrective action should be taken as soon as practical and cost effective. These recommendations concern actions where the implementation needs to be reviewed to determine if they are practical or cost effective or are beyond the direct control of the system owner and require implementation action by other NRC offices or external agencies. Certification of the system should not be delayed pending resolution of *Low Priority* actions. Nevertheless, they should be closely monitored to ensure that they are implemented as soon as practical and cost effective.

Upon request, approximately two (2) hours of assistance shall be provided to the NRC AMS System Owner to discuss the *Security Test & Evaluation (ST&E) Test Report* to correct deficiencies identified in the testing process.

The Contractor shall develop a *System Test & Evaluation (ST&E) Test Report* for the NRC AMS.

#### **2.2.3.4 Milestone 3-4: Develop a Business Continuity Plan for the AMS**

The Contractor shall develop a *Business Continuity Plan* for the NRC AMS in accordance with the *Project Management Plan* prepared and approved in Milestone 1. The plan shall detail procedures for NRC to respond to and recover from operational disasters and shall identify components necessary to provide the support required to continue operations in the event of a disaster. The Contractor shall review system documentation and interview cognizant NRC personnel to identify tasks required to resume emergency-level and full operations related to the NRC AMS; shall determine requirements for restoration of the system to include personnel, hardware, software, media, supplies, facilities, communications, and transportation; shall identify sources for meeting requirements; and shall document recovery strategies. The Contractor shall provide Living Disaster Recovery Planning System (LDRPS) certified personnel to document the AMS business continuity information within the NRC's LDRPS application.

The Contractor shall develop a Draft and Final *Business Continuity Plan* for the NRC AMS.

#### **2.2.3.5 Milestone 3-5: Develop the System Certification Report for the AMS**

The Contractor shall develop a *System Certification Report* for the NRC AMS in accordance with the *Project Management Plan* prepared and approved in Milestone 1 that shall summarize the results of each step of this milestone. Preparation of certification statements, all worksheets, and documentation required by FIPS Publication 102 shall be submitted for the certification of the NRC AMS.

The *System Certification Report* for the NRC AMS shall include the Risk Assessment Report, System Security Plan, Certification Letter, and Worksheets 1 through 6 from the DOC Abbreviated Certification Methodology. It shall contain recommendations for improvements and recommendations to the accrediting official. The *System Certification Report* shall be prepared in accordance with the Computer Security Act of 1987, Federal statutes and regulations, as well as NRC Management Directives.

The Contractor shall develop the *System Certification Report* for the NRC AMS.

#### **2.2.4 Milestone 4: Operator Licensing Tracking System (OLTS) (OPTIONAL)**

The Contractor shall perform data collection, interviews, and documentation review and analysis

in accordance with the *Project Work Plan* prepared and approved in Milestone 1. Approximately five (5) to ten (10) detailed interviews are anticipated with NRC employees and Contractor personnel located in Rockville, MD. This milestone is divided into four (4) subtasks, with the possibility of adding one (1) additional subtask at a later date.

#### **2.2.4.1 Milestone 4-1: Develop a Risk Assessment Report for the OLTS**

The Contractor shall coordinate with OCIO management to schedule potential interviews with identified key Agency personnel familiar with the management, operations, and security of the system. The Contractor shall utilize this information to assess the current operating environment, concentrating on analysis of data sensitivity, and identification of threats and vulnerabilities to the NRC OLTS system. Based on the results and analysis of interviews and data collection efforts, the Contractor shall conduct a risk assessment of the NRC OLTS operating environment, and develop a *Risk Assessment Report* for the NRC OLTS.

The objectives of this risk assessment for the NRC OLTS shall be to:

- Identify potential undesirable or unauthorized events;
- Identify risks that could have a negative impact on the confidentiality, integrity, or availability of information processed or stored by, or transmitted through the system;
- Identify potential controls to reduce or eliminate the impact of risk events; and
- Establish responsibilities and milestones for the implementation of mitigating controls.

The Contractor shall document the results of this process. This shall include documenting the risk number; a description of each risk; the type of risk (i.e., impacting the confidentiality, integrity, or availability of an asset); the level of concern (i.e., major or minor); the associated controls; and the action(s) required to minimize each risk.

The Contractor shall develop a Draft and Final *Risk Assessment Report* for the NRC OLTS.

#### **2.2.4.2 Milestone 4-2: Develop the System Security Plan for the OLTS**

Based on the results and analysis of interviews and data collection efforts, the Contractor shall develop the *System Security Plan* for the NRC OLTS. This plan shall follow the format of NIST SP 800-18, that shall be used as a foundation for the analysis and presentation of essential security plan information. Plan development shall also include a preliminary estimation of the status of necessary safeguards (i.e., in-place, planned, in-place and planned, or not applicable).

As necessary, the Contractor shall develop a set of application Rules of Behavior for inclusion in the *System Security Plan* to ensure compliance with NIST SP 800-18.

The Contractor shall develop the Draft and Final *System Security Plan* for the NRC OLTS.

#### **2.2.4.3 Milestone 4-3: Develop the Security Test & Evaluation (ST&E) Test Plan and Report for the OLTS**

The Contractor shall develop a *Security Test & Evaluation (ST&E) Test Plan* for the OLTS in accordance with the *Project Management Plan* prepared and approved in Milestone 1. Additionally, the Contractor shall perform security testing conducted with NRC personnel and shall prepare a *Security Test & Evaluation (ST&E) Test Report* for the NRC OLTS. This milestone is divided into two (2) subtasks.

##### **Milestone 4-3-1: Develop the Security Test & Evaluation (ST&E) Test Plan**

The Contractor shall develop a test plan for reviewing and testing the security control measures protecting the NRC OLTS using the DOC Abbreviated Certification Methodology. The deliverable shall include plans for testing the adequacy of system security safeguards.

The Contractor shall develop a *System Test & Evaluation (ST&E) Test Plan* for the NRC OLTS.

##### **Milestone 4-3-2: Develop the Security Test & Evaluation (ST&E) Test Report**

The Contractor shall conduct system testing of safeguards for the NRC OLTS and provide recommendations for improvements to the system using the *System Security Plan* developed in Milestone 4-3 and the *System Test & Evaluation (ST&E) Test Plan* developed in Milestone 4-3-1. Recommendations for improvements to the NRC OLTS shall be made upon evaluation of the system test results, and shall be incorporated into a *Security Test & Evaluation (ST&E) Test Report*. Each safeguard shall be categorized as follows:

**High Priority:** Corrective action should be taken prior to formal certification of the system. Expedient implementation of *High Priority* recommendations is based on the criticality of the affected safeguards to the security of the system. A plan of action for mitigating the situation and implementing corrective actions should be developed and approved by NRC management within thirty (30) days of receipt of the report.

**Moderate Priority:** Though important to enhancing the security of the system, corrective action of *Moderate Priority* risks should be taken irrespective of formal system certification. Where practical and cost effective, these recommendations should be implemented within six (6) months.

**Low Priority:** Corrective action should be taken as soon as practical and cost effective. These recommendations concern actions where the implementation needs to be reviewed to determine if they are practical or cost effective or are beyond the direct control of the system owner and require implementation action by other NRC offices or external agencies. Certification of the system should not be delayed pending resolution of *Low Priority* actions. Nevertheless, they should be closely monitored to ensure that they are implemented as soon as practical and cost effective.

Upon request, approximately two (2) hours of assistance shall be provided to the NRC OLTS System Owner to discuss the *Security Test & Evaluation (ST&E) Test Report* to correct deficiencies identified in the testing process.

The Contractor shall develop a *System Test & Evaluation (ST&E) Test Report* for the NRC OLTS.

#### **2.2.4.4 Milestone 4-4: Develop a Business Continuity Plan for the OLTS**

The Contractor shall develop a *Business Continuity Plan* for the NRC OLTS in accordance with the *Project Management Plan* prepared and approved in Milestone 1. The plan shall detail procedures for NRC to respond to and recover from operational disasters and shall identify components necessary to provide the support required to continue operations in the event of a disaster. The Contractor shall review system documentation and interview cognizant NRC personnel to identify tasks required to resume emergency-level and full operations related to the NRC OLTS; shall determine requirements for restoration of the system to include personnel, hardware, software, media, supplies, facilities, communications, and transportation; shall identify sources for meeting requirements; and shall document recovery strategies. The Contractor shall provide Living Disaster Recovery Planning System (LDRPS) certified personnel to document the OLTS business continuity information within the NRC's LDRPS application.

The Contractor shall develop a Draft and Final *Business Continuity Plan* for the NRC OLTS.

#### **2.2.4.5 Milestone 4-5: Develop the System Certification Report for the OLTS**

The Contractor shall develop a *System Certification Report* for the NRC OLTS in accordance with the *Project Management Plan* prepared and approved in Milestone 1 that shall summarize the results of each step of this milestone. Preparation of certification statements, all worksheets, and documentation required by FIPS Publication 102 shall be submitted for the certification of the NRC OLTS.

The *System Certification Report* for the NRC OLTS shall include the Risk Assessment Report, System Security Plan, Certification Letter, and Worksheets 1 through 6 from the DOC Abbreviated Certification Methodology. It shall contain recommendations for improvements and recommendations to the accrediting official. The *System Certification Report* shall be prepared in accordance with the Computer Security Act of 1987, Federal statutes and regulations, as well as NRC Management Directives.

The Contractor shall develop the *System Certification Report* for the NRC OLTS.

#### **2.2.5 Milestone 5: Exit Briefing Presentation**

During this milestone, the Contractor shall conduct an *Exit Briefing Presentation* with NRC staff in accordance with the *Project Management Plan* prepared and approved in Milestone 1. The presentation shall include a brief summary of the work performed and documents prepared, and answer NRC staff questions.

The Contractor shall develop an *Exit Briefing Presentation* for the NRC NRR task.

### **3.0 Reporting Requirements**

#### **3.1 Monthly Technical Progress Reports**

The contractor shall provide a Monthly Technical Progress Report to the Project Officer and the Contracting Officer. The report is due the 15<sup>th</sup> of each month and must identify the title of the project, the delivery order number, Financial Identification Number (FIN), project manager and/or principal investigator, the delivery order period of performance, and the period covered by the report. Each report must include the following:

- a. a listing of the efforts completed during the period, by individual's name, and milestones reached, or, if missed, an explanation provided;
- b. Progress reports shall cover all work completed during the preceding month and shall present the work to be accomplished during the subsequent month. This report shall also identify any problems or delays encountered or anticipated and recommendations for resolution. If the recommended resolution involves a delivery order modification, e.g., change in work requirements, level of effort (cost) or schedule delay, the contractor shall submit a separate letter to the contracting officer identifying the required change and estimated cost impact.

#### **3.2 Monthly Financial Status Report**

The Contractor shall provide a Monthly Financial Status Report to the Project Officer and Contracting Officer. The report is due the 15<sup>th</sup> of each month and must identify the title of the project, the delivery order number, Financial Identification Number (FIN), project manager and/or principal investigator, the delivery order period of performance, and the period covered by the report. Each report must include the following for each task:

- (a) Provide total estimated cost (value) of the project as reflected in the delivery order, the amount of funds available in the delivery order to date, and the balance of funds required to complete the work as follows:
  1. Total estimated delivery order amount.
  2. Total costs incurred this reporting period.
  3. Total costs incurred to date.
  4. Balance of funds required to complete the delivery order.
- (b) Projected percentage of completion cumulative through the report period for the project as reflected in the current CSP.
  1. Indicate if there has been a significant change in the original CSP projection in either dollars or percentage of completion. Identify the change, the reasons for the change, whether there is any projected overrun, and when additional funds would be required. If there have been no changes to the original NRC-approved CSP projections, a written statement to that effect is sufficient in lieu of submitting a detailed response.
- (c) A revised CSP is required with the Financial Status Report whenever the Contractor or the Contracting Officer has reason to believe that the total cost for performance of this delivery order will be either greater or substantially less than what had been previously estimated.
- (d) If the data in this report indicates a need for additional funding beyond that already obligated, this information may only be used as support to the official report for funding required

in accordance with Clause (FAR 52.232-1), Payments Clause, which is hereby incorporated and made a part of this delivery order.

### **3.3. Place of Delivery-Reports**

The items to be furnished hereunder shall be delivered to the individuals reflected below, with all charges paid by the contractor and shall be provided by the established delivery date:

(a) Name: Louis Numkin, Project Officer (2 copies)

Address: OCIO/ADD/CSS MS-T7-F5

Washington DC, 0555

Name: Mark Flynn, Contracting Officer (1 copy)

Address: MS T7-I2

Washington, DC 20555

### **4.0 52.242-15 Stop Work Order**

(a) The Contracting Officer may, at any time, by written order to the contractor, require the contractor to stop all, or any part, of the work called for by this delivery order for a period of 90 days after the order is delivered to the contractor, and for any further period to which the parties may agree. The order shall be specifically identified as a stop-work order issued under this clause. Upon receipt of the order, the contractor shall immediately comply with its terms and take all reasonable steps to minimize the incurrence of costs allocable to the work covered by the order during the period of work stoppage. Within a period of 90 days after a stop-work order is delivered to the contractor, or within any extension of that period to which the parties shall have agreed, the Contracting Officer shall either - (1) Cancel the stop-work order; or

(2) Terminate the work covered by the order as provided in the Default, or the Termination for Convenience of the Government, clause of this delivery order.

(b) If a stop-work order issued under this clause is canceled or the period of the order or any extension thereof expires, the contractor shall resume work. The Contracting Officer shall make an equitable adjustment in the delivery schedule or delivery order price, or both, and the delivery order shall be modified, in writing, accordingly, if- (1) The stop-work order results in an increase in the time required for, or in the contractor's cost properly allocable to, the performance of any part of this delivery order; and (2) The Contractor asserts its right to the adjustment within 30 days after the end of the period of work stoppage; provided, that, if the Contracting Officer decides the facts justify the action, the Contracting Officer may receive and act upon a proposal submitted at any time before final payment under this delivery order.

(c) If a stop-work order is not canceled and the work covered by the order is terminated for the convenience of the Government, the Contracting Officer shall allow reasonable costs resulting from the stop-work order in arriving at the termination settlement.

(d) If a stop-work order is not canceled and the work covered by the order is terminated for default, the Contracting Officer shall allow, by equitable adjustment or otherwise, reasonable costs resulting from the stop-work order.

**5.0 Milestones and Deliverables**

The orientation meeting shall be held no later than five (5) days from the date of the task award. During this meeting, discussion shall include the five (5) milestones and corresponding deliverables as identified in Section 2.0 Proposal Solution, above.

The Contractor shall deliver three (3) copies of all earlier specified deliverables to the NRC Client Representative during normal business hours. Final deliverables (except Monthly Status Reports) shall also be made electronically available in Corel WordPerfect 8 format on a 3.5 inch virus-free diskette or CD-ROM. The NRC shall have ten (10) working days to review Draft deliverables and five (5) working days to review Final deliverables, and to accept or reject the deliverable in writing.

In addition to the formal deliverables, the Contractor shall conduct, at a minimum, one (1) meeting every two (2) weeks between the Contractor and key client personnel. The meeting shall take place at the Client Representative's Office. Based on the client's work schedule, this meeting can be held by phone at the request of the client.

<b>SCHEDULE OF DELIVERABLES</b>				
<b>DELIVERABLE</b>	<b>MS</b>	<b>DELIVERABLE DESCRIPTION</b>	<b>NO. OF COPIES</b>	<b>DATE DUE</b>
1	1	Draft <i>Project Management Plan</i> for the NRC NRR task.	3	TBD
	1	Final <i>Project Management Plan</i> for the NRC NRR task.	3	TBD
2	2-1	Draft Risk Assessment Report for RPS	3	TBD
2	2-1	Final Risk Assessment Report for RPS	3	TBD
3	2-2	Draft System Security Plan for RPS	3	TBD
3	2-2	Final System Security Plan for RPS	3	TBD
4	2-3-1	System Test and Evaluation Test Plan for RPS	3	TBD
5	2-3-2	System Test and Evaluation Test Report for RPS		
6	2-4	Draft Business Continuity Plan for RPS		
	2-4	Final Business Continuity Plan for RPS		
7	2-5	System Certification Report for RPS		
8	3-1	Draft Risk Assessment Report for AMS		
		Final Risk Assessment Report for AMS		

	3-2	Draft System Security Plan for AMS		
		Final System Security Plan for AMS		
	3-3-1	System Test and Evaluation Test Plan for AMS		
	3-3-2	System Test and Evaluation Test Report for AMS		
	3-4	Draft Business Continuity Plan for AMS		
		Final Business Continuity Plan for AMS		
	3-5	System Certification Report for AMS		
		Monthly Status Report	3	15 <sup>th</sup> of the month
		Financial Status Report	3	15 <sup>th</sup> of the month
	4-1 TO 4- 5	OPTIONAL DELIVERABLE DUE DATES FOR OLTS WILL BE PROVIDED WHEN OPTION EXERCISED		

## 6.0 Period Of Performance

"The period of performance for the base period is estimated to be 8 months from the award of this contract. The option period is anticipated to be 4 month if exercised under this delivery order."

The period of performance for this delivery order is from the date of award through March 31, 2001.

## 7.0 Travel

Local travel from the Contractor office to NRC HQ in Rockville, MD is anticipated and shall be conducted in accordance with the NRC SOW. No travel outside the Metropolitan Washington, D.C. area shall be conducted.

## 8.0 Security

(a) Security/Classification Requirements Form. The attached NRC Form 187 (Attachment 1) 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 information or matter, access on a continuing basis (in excess of 30 or more days) to NRC Headquarters controlled buildings, or otherwise requires NRC photo identification or card-key badges.

(b) It is the contractor's duty to safeguard 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 safeguarding 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

delivery order 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 delivery order 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, proprietary data (trade secrets) 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 agrees to hold the information in confidence and not to 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 and the Contracting Officer. These changes will be under the authority of the FAR Changes clause referenced in this document.

(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) Security Clearance Personnel. 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.

(i) 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.)

(j) 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.

(k) In performing the delivery order 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.

#### **SITE ACCESS BADGE REQUIREMENTS**

During the life of this contract, the rights of ingress and egress for contractor personnel must be made available, as required, provided that a badge is issued after favorable adjudication from the Personnel Security Branch, Division of Facilities and Security (PERSEC/DFS). In this regard, all contractor personnel whose duties under this delivery order 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 a proper Government-issued identification/badge at all times. All prescribed identification must be immediately (no later than three days) delivered to PERSEC/DFS 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 delivery order work, and to assure the safeguarding of any Government records or data that contractor personnel may come into contact with.

#### **SECURITY REQUIREMENTS FOR INFORMATION TECHNOLOGY SERVICES**

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.

#### **CONTRACTOR SECURITY REQUIREMENTS FOR LEVEL I**

Performance under this delivery order 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 NRC facilities, sensitive information technology systems or data until he/she is approved by Personnel Security Branch, Division of Facilities and Security (PERSEC/DFS) first for temporary access (based on a favorable adjudication of their security forms and checks) and final access (based on a favorably adjudicated LBI) in accordance with the procedures found in NRC MD 12.3, Part I. The individual will be subject to a reinvestigation every 10 years. **Timely receipt of properly completed security applications is a delivery order 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.

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 PERSEC/ 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 delivery order by reference as though fully set forth herein. Based on PERSEC 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 Exhibit 1 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 and 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 NRC photo identification or card-key badges.

## CONTRACTOR SECURITY REQUIREMENTS FOR LEVEL II

Performance under this delivery order will involve contractor personnel that develop and/or analyze sensitive information technology systems or data or otherwise have access to such systems and 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 delivery order 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 NRC facilities, sensitive information technology systems or data until he/she is approved by PERSEC/DFS first for temporary access (based on a favorable review of their security forms and checks) and final access (based on a favorably adjudicated ANACI) in accordance with the procedures found in MD 12.3, Part I. The individual will be subject to a reinvestigation every 10 years. Timely receipt of properly completed security applications is a delivery order 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.

**The contractor shall submit a completed security forms packet (enclosed), including the SF-86, "Questionnaire for National Security Positions," and fingerprint charts, through the Project Officer to the NRC PERSEC/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 PERSEC 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 Exhibit 1 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 and 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 NRC photo identification or card-key badges.

## 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 contact the PERSEC/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 to the PERSEC/DFS. Additionally, PERSEC/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.

## **9.0 Project Officer Authority**

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

Name: Louis Numkin

(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, authorizes travel which was unanticipated in the Schedule (i.e., travel not contemplated in the Statement of Work or changes to specific travel identified in the Statement of Work), 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, approval of 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 blanket purchase agreement.

(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) All technical directions must be issued in writing by the project officer or must be confirmed by the project officer in writing within ten (10) working days after verbal issuance. A copy of the written direction must be furnished to the contracting officer. A copy of NRC Form 445, Request for Approval of Official Foreign Travel, which has received final approval from the NRC must be furnished to the contracting officer.

(e) 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.

(f) 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.

(g) 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.

(h) 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.

(i) 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.

## **10. Government-Furnished Materials**

The NRC Technical Project Officer will furnish to the contractor all necessary standards documents and guidance materials required for compliance with the conditions outlined in this Statement of Work.

1. NRC Management Directive 12.5, "NRC Automated Information Systems Security Program"

2. The Insider Threat To U.S. Government Information Systems, NSTISSAM INFOSEC/1-99, July 1999
3. Mitigating risks to the Insider Threat within your Organization, Harry Krimkowitz, October 24, 2000, the SANS institute

The Insider Threat To Information Systems, Eric D. Shaw, Ph.D., and others.

#### **11. Kick-Off Meeting**

A kick-off meeting will be held to introduce the NRC Project Officer and the Technical Project Officer.