

**ORDER FOR SUPPLIES OR SERVICES**

**IMPORTANT:** Mark all packages and papers with contract and/or order numbers. BPA NO.

1. DATE OF ORDER 07-12-2004	2. CONTRACT NO. (if any) GS-35F-0079J	6. SHIP TO:
ORDER NO. NRC-33-01-191-009	MODIFICATION NO.	4. REQUISITION/REFERENCE NO. NRC030409, dtd4/8/04
3. ISSUING OFFICE (Address correspondence to) U.S. Nuclear Regulatory Commission Division of Contracts Contract Management Center 1  Washington, DC 20555-0001		5. NAME OF CONSIGNEE U.S. Nuclear Regulatory Commission Office of the Chief Information Officer

b. STREET ADDRESS ATTN: Louis M. Numkin Mail Stop: T-6-F15		c. CITY Washington	d. STATE DC	e. ZIP CODE 20555-0001
--	--	-----------------------	----------------	---------------------------

7. TO: I. SHIP VIA

NAME OF CONTRACTOR  ALLIED TECHNOLOGY GROUP, INC. ATTN: William P. Connor Senior Vice President 1803 Research Boulevard, Suite 601  Rockville MD 20850  <i>Timothy F. Wynne 7/14/04</i> <b>TIMOTHY F. WYNNE, VICE PRESIDENT</b>		8. TYPE OF ORDER  <input type="checkbox"/> a. PURCHASE ORDER 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.  <input checked="" type="checkbox"/> b. DELIVERY/TASK ORDER 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.	
---	--	--	--

ACCOUNTING AND APPROPRIATION DATA B&R NO.: 420-15-101-160, JOB CODE: J3123, BOC: 3131 APPN. NO.: 31X0200.420, OBLIGATE: \$21,736.42	10. REQUISITIONING OFFICE  Office of the Chief Information Officer
---	--

9. BUSINESS CLASSIFICATION (Check appropriate box(es))

a. SMALL       b. OTHER THAN SMALL       c. DISADVANTAGED       d. WOMEN-OWNED

11. F.O.B. POINT N/A	14. GOVERNMENT B/L NO.	15. DELIVER TO F.O.B. POINT ON OR BEFORE Refer to the SOW.	16. DISCOUNT TERMS N/A
-------------------------	------------------------	--	---------------------------

13. PLACE OF      FOR INFORMATION CALL: (No collect calls)

INSPECTION Destination	b. ACCEPTANCE Destination	Donald A. King Office: (301) 415-6731
---------------------------	------------------------------	--

17. SCHEDULE (See reverse for Rejections)

TEM NO. (A)	SUPPLIES OR SERVICES (B)	QUANTITY ORDERED (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)	QUANTITY ACCEPTED (G)
	<p>The U. S. Nuclear Regulatory Commission (NRC) hereby accepts the quotation of Allied Technology Group, Inc. (Allied), dated May 27, 2004, which is hereby incorporated by reference and made a part hereof this delivery order, to provide the NRC with computer security services for its Computer Security Review/Update of the NRR RPS System, at the firm fixed unit price reflected in the Schedule of Prices/Costs for each task.</p> <p>TIN: 52-1603280 DUNS NO.: 62-122-5598</p> <p>NRC Project Officer - Louis M. Numkin - (301) 415-5906</p>					

18. SHIPPING POINT	19. GROSS SHIPPING WEIGHT	20. INVOICE NO.	\$21,736.42	SUBTOTAL
21. MAIL INVOICE TO:				17(h) TOTAL (Cont. pages)
a. NAME U.S. Nuclear Regulatory Commission Division of Contracts				17(i) GRAND TOTAL
b. STREET ADDRESS (or P.O. Box) Attn: Donald A. King Mail Stop: T-7-12				
c. CITY Washington	d. STATE DC	e. ZIP CODE 20555-0001	21,736.42	

UNITED STATES OF AMERICA BY (Signature)  <i>Donald A. King</i>	23. NAME (Typed) Donald A. King Contracting Officer TITLE: CONTRACTING/ORDERING OFFICER
---	--

CONTINUATION PAGE

**A.1 ADDENDA - SCHEDULE OF SUPPLIES OR SERVICES AND PRICE/COSTS**

**1      PROJECT TITLE**

The title of this project is as follows:

**"COMPUTER SECURITY REVIEW/UPDATE OF THE NRR RPS SYSTEM"**

**2.      BRIEF DESCRIPTION OF WORK**

**a) Brief description of work:**

The U.S. Nuclear Regulatory Commission requires contractor support to provide: (1) identify the most cost-effective security solutions that can be incorporated within the existing NRC network infrastructure; (2) provide the capability for NRC users to securely process and exchange sensitive information, both internally and with external customers; and (3) provide expert level security engineering technical support to the NRC, to assist in the analysis and assessment of security issues and problems associated with the existing NRC local area network infrastructure; for the Office of the **Chief Information Officer (OCIO)**.

**(b)** Only Contracting Officers of the NRC or other individuals specifically authorized under this task order may authorize the initiation of work under this task order. The provisions of this task order shall govern all required work hereunder.

**3.      SCHEDULE**

The Contractor shall provide **security technology assessment** support services to NRC in accordance with the "DESCRIPTION/SPECIFICATIONS/WORK STATEMENT" for the task order period of performance at the rates as set forth below.

NRC-33-01-191-009 SECTION A

SCHEDULE OF SERVICES

CLIN 0001 -TASK 1 ORIENTATION MEETING

Labor Category	Rate \$	Hours	Dollars
Project Manager 206C	[REDACTED]	[REDACTED]	\$469.12
Sr. Systems Analyst 205C	[REDACTED]	[REDACTED]	\$312.76
Sr. Systems Analyst 205C	[REDACTED]	[REDACTED]	\$0
Subtotal			\$781.88

CLIN 0002 - TASK 2 FINAL PROJECT MANAGEMENT PLAN

Labor Category	Rate	Hours	Dollars
Project Manager	[REDACTED]	[REDACTED]	\$469.12
Sr. Systems Analyst	[REDACTED]	[REDACTED]	\$625.52
Sr. Systems Analyst	[REDACTED]	[REDACTED]	\$0.00
Subtotal		[REDACTED]	\$1,094.64

CLIN 0003 - TASK 3 DRAFT RISK ASSESSMENT REPORT

Labor Category	Rate	Hours	Dollars
Project Manager	[REDACTED]	[REDACTED]	\$2,814.72
Sr. Systems Analyst	[REDACTED]	[REDACTED]	\$1,876.56
Sr. Systems Analyst	[REDACTED]	[REDACTED]	\$625.52
Subtotal		[REDACTED]	\$5,316.80

**NRC-33-01-191-009 SECTION A**

**CLIN 0004 - TASK 4 FINAL RISK ASSESSMENT REPORT**

<b>Labor Category</b>	<b>Rate</b>	<b>Hours</b>	<b>Dollars</b>
Project Manager	[REDACTED]	[REDACTED]	\$469.12
Sr. Systems Analyst	[REDACTED]	[REDACTED]	\$1,251.04
Sr. Systems Analyst	[REDACTED]	[REDACTED]	\$156.38
Subtotal		[REDACTED]	\$1,876.54

**CLIN 0005 - TASK 5 DRAFT SYSTEM SECURITY PLAN**

<b>Labor Category</b>	<b>Rate</b>	<b>Hours</b>	<b>Dollars</b>
Project Manager	[REDACTED]	[REDACTED]	\$938.24
Sr. Systems Analyst	[REDACTED]	[REDACTED]	\$1,251.04
Sr. Systems Analyst	[REDACTED]	[REDACTED]	\$312.76
Subtotal		[REDACTED]	\$2,502.04

**CLIN-0006 - TASK 6 FINAL SYSTEM SECURITY PLAN**

<b>Labor Category</b>	<b>Rate</b>	<b>Hours</b>	<b>Dollars</b>
Project Manager	[REDACTED]	[REDACTED]	\$469.12
Sr. Systems Analyst	[REDACTED]	[REDACTED]	\$625.52
Sr. Systems Analyst	[REDACTED]	[REDACTED]	\$0.00
Subtotal			\$1,094.64

**NRC-33-01-191-009 SECTION A**

**CLIN 0007 - TASK 7 SECURITY TEST & EVALUATION (ST&E) PLAN**

Labor Category	Rate	Hours	Dollars
Project Manager	[REDACTED]	[REDACTED]	\$938.24
Sr. Systems Analyst	[REDACTED]	[REDACTED]	\$1,251.04
Sr. Systems Analyst	[REDACTED]	[REDACTED]	\$625.52
Subtotal		[REDACTED]	\$2,814.80

**CLIN 0008 - TASK 8 SECURITY TEST & EVALUATION (ST&E) REPORT**

Labor Category	Rate	Hours	Dollars
Project Manager	[REDACTED]	[REDACTED]	\$469.12
Sr. Systems Analyst	[REDACTED]	[REDACTED]	\$312.76
Sr. Systems Analyst	[REDACTED]	[REDACTED]	\$0.00
Subtotal		[REDACTED]	\$781.88

**CLIN-0009 - TASK 9 DRAFT IT CONTINGENCY PLAN**

Labor Category	Rate	Hours	Dollars
Project Manager	[REDACTED]	[REDACTED]	\$938.24
Sr. Systems Analyst	[REDACTED]	[REDACTED]	\$1,251.04
Sr. Systems Analyst	[REDACTED]	[REDACTED]	\$312.76
Subtotal		[REDACTED]	\$2,502.04

**NRC-33-01-191-009 SECTION A**

**CLIN 0010 - TASK 10 FINAL IT CONTINGENCY PLAN**

Labor Category	Rate	Hours	Dollars
Project Manager	[REDACTED]	[REDACTED]	\$469.12
Sr. Systems Analyst	[REDACTED]	[REDACTED]	\$312.76
Sr. Systems Analyst	[REDACTED]	[REDACTED]	\$0.00
Subtotal		[REDACTED]	\$781.88

**CLIN 0011 - TASK 11 IT CONTINGENCY PLAN TRAINING**

Labor Category	Rate	Hours	Dollars
Project Manager	[REDACTED]	[REDACTED]	\$938.24
Sr. Systems Analyst	[REDACTED]	[REDACTED]	\$1,251.04
Sr. Systems Analyst	[REDACTED]	[REDACTED]	\$0.00
Subtotal		[REDACTED]	\$2,189.28

**TOTAL ALL TASKS** **\$21,736.42**

The fixed unit price of each line item shown above to meet requirements as delineated in Section entitled "Statement of Work," shall include all cost deemed necessary by the offeror.

**A.2 CONSIDERATION AND OBLIGATION**

(a) The total estimated amount of this contract(ceiling) for the products/services ordered, delivered, and accepted under this contract is **\$21,736.42**. The Contracting Officer may unilaterally increase this amount as necessary for orders to be placed with the contractor during the contract period provided such orders are within any maximum ordering limitation prescribed under this contract.

(b) The amount presently obligated with respect to this contract is **\$21,736.42**. The Contracting Officer may issue orders for work up to the amount presently obligated. This obligated amount may be unilaterally increased from time to time by the Contracting Officer by written modification to this contract. The obligated amount shall, at no time, exceed the contract ceiling as specified in paragraph (a) above. 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.

**NRC-33-01-191-009 SECTION A**

**A.3 PERIOD OF PERFORMANCE**

The period of performance for this delivery order is from the date of award through December 31, 2004.

**A.4 SCHEDULE OF DELIVERABLES**

Each deliverable line in this schedule of deliverables table has two (2) appended columns: "T+#" gives the number of expected work days required for the line items completion from project award date.

"Required date" maximum completion dates already determined by NRR.

Deliverable #	Milestone	Deliverable Title	T+#	Required Date
1	1	Orientation Meeting	-	With 5 days of task award.
2	1	Final Project Management Plan	T+10	7/26/04
3	2	Draft Risk Assessment Report	T+40	9/7/04
4	2	Final Risk Assessment Report	T+55	9/28/04
5	3	Draft System Security Plan	T+50	9/21/04
6	3	Final System Security Plan	T+105	12/6/04
7	4	Security Test & Evaluation (ST&E) Plan	T+60	10/5/04
8	4	Security Test & Evaluation (ST&E) Report	T+75	10/27/04
9	5	Draft IT Contingency Plan	T+70	10/20/04
10	5	Final IT Contingency Plan	T+100	11/29/04
11	6	IT Contingency Plan Training	T+85	11/4/04
12	7	IT Contingency Plan Test Plan	T+75	10/27/04
13	7	IT Contingency Plan Test Report	T+90	11/12/04
14	8	System Certification/Accred Report	T+115	12/20/04
15	9	Draft Self Assessment	T+100	11/29/04
16	9	Draft Action Plan	T+100	11/29/04
17	9	Final Self Assessment	T+110	12/13/04
18	9	Final Action Plan	T+110	12/13/04
19	10	Exit Briefing Presentation for RPS	T+120	12/28/04

## A.5 DESCRIPTION/SPECIFICATIONS/WORK STATEMENT

### 1.0 BACKGROUND

The Contractor shall provide computer security services to the U.S. Nuclear Regulatory Commission (NRC), to both NRR and to the Office of Chief Information Officer (OCIO), for the Reactor Program System (RPS).

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.

In accordance with the Office of Management and Budget (OMB) Circular A-130, Appendix III, *Security of Federal Automated Information Resources* and the Federal Information Security Management Act (FISMA), the NRC is required to perform risk assessments, develop system security plans, develop security test and evaluation plans, perform testing of security controls, develop information technology (IT) contingency plans, provide IT contingency plan training to personnel, develop test plans for IT contingency plans, perform testing of IT contingency plans, and develop a system certification report for its information resources.

The NRC requires the support of a Contractor to review and update the appropriate security documentation for the RPS, to ensure compliance with current Federal guidelines. The system requires the following items be reviewed and updated: a Risk Assessment Report, a System Security Plan (SSP), a Security Test & Evaluation (ST&E) Plan, security controls testing, an ST&E Report, an IT Contingency Plan, IT Contingency Plan training, IT Contingency Plan testing, an IT Contingency Plan Test Report, a System Re-Certification Report, and a Security Self-Assessment (Appendix A) of the Self-Assessment Guide for Information Technology Systems (NIST Special Publication 800-26).

The Risk Assessment Report, System Security Plan (SSP), Security Test & Evaluation (ST&E) Plan, security controls testing, ST&E Report, Business Continuity Plan and System Certification Report which were completed between October and December 2001 are available in electronic form from the NRC Project Officer. Only minor changes have been made to RPS and the NRC IT environment since that time. A Security Self-Assessment (Appendix A) of the Self-Assessment Guide for Information Technology Systems (NIST Special Publication 800-26) for RPS was completed in 2003 and is available in electronic form from the Project Officer. It is envisioned that these documents should be reviewed and revised, if needed, to insure that they are in compliance with the latest security directives and policy.

### 1.1 SYSTEM DESCRIPTION

RPS, a Major Application, was initiated in 1995, when NRR recognized the need to gain

regulatory and administrative improvements and efficiencies. NRR initiated the program with the OCIO 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 OCIO. Many of these older systems did not effectively interface or share information resulting in inefficiencies that impeded 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 NRC 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 thirteen (13) modules of the RPS covered by this plan are:

- Inspection Planning (IP) module
- Time Resource Inventory Management (TRIM) module
- Inspection Planning Cycle (IPC) module
- Inspection Procedure Authority System (IPAS) module
- Inspection Report Tracking System (IRTS) module
- Item Reporting (IR) module
- Security Access Method (SAM) module
- TABLES module
- Reports module
- Performance Measures (PM) module
- Reactor Oversight Process (ROP) module
- NRC Utilities (NRCUTIL) module
- Safety Issues Management System (SIMS) module

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. 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 Reactor Program.

## 1.2 SYSTEM ENVIRONMENT

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 under Windows) using COTS software for greater flexibility and ease of maintenance. The system provides inherent staff efficiencies and improved data quality through several means that 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, 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 IBM RS/6000s) installed in HQ and each region. Data replication is used to maintain data integrity across the network of IBM 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.

The RPS database is implemented using SYBASE Adaptive Server Environment (ASE) Version 12.0.0.5 relational database management system (RDBMS) software and is located on a file server within HQ offices, as well as the Regional Offices. The RPS can be accessed via modem as in the case of Regional Resident Inspectors or via direct connectivity for individuals in HQ or the Regional Offices. The RPS database uses an IBM RS/6000 server as its hardware platform and IBM's UNIX-based AIX 4.3.3 as its operating system. The AIX is used as a database machine and only has SYBASE and root installed, with no general user access authorized. SYBASE ASE Version 12.0.0.5 RDBMS is capable of providing database support for the enterprise resource planning needs of the potentially geographically dispersed clients of the RPS.

Dial-up access to the RPS is based on Citrix MetaFrame running on a Windows NT platform. A user has the Citrix ICA client on their remote PC, dials into a Nortel 5399 Remote Annex device to establish a point-to-point protocol (PPP) session, and logs onto the Citrix servers, owned by OCIO. Regional Resident inspectors have direct linkage through their Regional Office and only use the Citrix when on travel.

### **1.7.2 Infrastructure-Specific System Environment**

The RPS is supported by two (2) Data Centers, one (1) located in OWFN and the other in TWFN. The Data Centers are managed by the OCIO, Infrastructure and Computer Operations Division (ICOD), Computer Operations and Telecommunications (COTB). Application-specific servers located within the Data Centers are maintained by OCIO/ICOD/COTB. Both Data Centers are categorized as a General Support System:

The OWFN Data Center is located in Room O-2-G-3 on the second floor at 11555 Rockville Pike, Rockville, MD. Tape backups generated in the TWFN Data Center are currently being stored in the OWFN Data Center. NRC is in the process of establishing an off-site storage facility with the Washington National Records Archives Center in Suitland, MD.

The TWFN Data Center is located in Room T-5-B-3 on the fifth floor at 11545 Rockville Pike, Rockville, MD. This Data Center supports the RPS production server (RPS5), the warm standby server (IRM63), the development server (IRM50), and the training server (IRM59).

The RPS application is connected to the NRC customer base through the NRC HQ local area network/wide area network (LAN/WAN) general support system (Agency infrastructure). The NRC HQ LAN system is actually a number of switched 100 Megabyte (MB) Ethernet segments tied together via routers. The two (2) buildings are connected via Asynchronous Transfer Mode (ATM) over fiber optic cables. Remote NRC and contractor sites are connected into NRC HQ

routers by a combination of dedicated T-1 and 256 Kilobits per second (Kbps) frame relay connections. Internet access is provided through a connection to the National Institutes of Health (NIH). Novell Netware 5 is the LAN operating system administering the NRC network that hosts the RPS. The NRC WAN connects the NRC network to the NRC Regional Offices across the country, the Technical Training Center in Chattanooga, TN and remote NRC offices in Washington, D.C. and Rockville, MD. The WAN also links the NRC network with project offices of NRC contractors. OCIO/ICOD/COTB operates all applications on the NRC infrastructure, therefore no service level agreements are required. OCIO is responsible for security aspects and training for the Agency infrastructure. Additional information about the NRC HQ LAN/WAN system can be obtained in the *Certification Report for the NRC Headquarters Local Area Network/Wide Area Network (LAN/WAN)*, dated July 27, 2001. A copy of this report is maintained by the OCIO Project Manager, Mr. Louis Numkin.

## **2.0 SCOPE OF WORK**

### **2.1 Plans for Performance**

NRC requires the Contractor to complete this project in ten (10) milestones and corresponding deliverables on a FFP basis. Each milestone consists of performing required tasks resulting in specific deliverables, as described below:

- Milestone 1: Develop a Project Management Plan for RPS Re-Accreditation
- Milestone 2: Update the Risk Assessment Report
- Milestone 3: Update the System Security Plan
- Milestone 4: Conduct Security Test & Evaluation
- Milestone 5: Update the IT Contingency Plan
- Milestone 6: Conduct IT Contingency Plan Training
- Milestone 7: Conduct IT Contingency Plan Testing
- Milestone 8: Develop a System Re-Certification and Re-Accreditation Report
- Milestone 9: Complete the Security Self-Assessment (Appendix A) of the Self-Assessment Guide for Information Technology Systems (NIST Special Publication 800-26)
- Milestone 10: Exit Briefing Presentation

The Contractor shall ensure that specifics pertaining to the system are fully addressed and that final deliverables can “stand-alone” serving as independent documents required for system certification.

## **2.2 TECHNICAL REQUIREMENTS**

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

The Contractor shall develop a *Project Management Plan* for RPS that details project milestones, deliverables, schedules, and management processes. The Contractor shall review pertinent published documentation, and based on this review, the Contractor shall formulate issues and questions necessary for interview sessions.

### **2.2.2 Milestone 2: Update the Risk Assessment Report**

The Contractor shall conduct a risk assessment of the RPS operating environment and shall develop an updated Draft and Final *Risk Assessment Report* for RPS. The Risk Assessment Report shall be completed following the guidance provided in NIST Special Publication (SP) 800-30, (Risk Management Guide for IT Systems). The objectives of this risk assessment for the RPS shall be to: identify potential undesirable or unauthorized events; identify risks that could have a negative impact on the integrity, confidentiality, 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 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, medium, or high), the associated controls, and the action(s) required to minimize each risk.

### **2.2.3 Milestone 3: Update the System Security Plan**

The Contractor shall develop an updated Draft and Final *System Security Plan* for RPS to be used on an interim basis until security testing is completed. This plan shall follow the format of NIST SP 800-18 and shall be used as a foundation for the analysis and presentation of essential security plan information. SSP development shall also include a preliminary estimation of the status of necessary safeguards.

Following the completion of security testing, the Contractor shall update the Draft *System Security Plan* for RPS to include lessons learned from security testing and shall submit a Final *System Security Plan*.

### **2.2.4 Milestone 4: Conduct Security Test & Evaluation**

The Contractor shall develop a *Security Test & Evaluation (ST&E) Plan* for RPS. The Contractor shall utilize the Department of Commerce (DOC) Abbreviated Certification Methodology Worksheets 1-4 to document the system description, identified vulnerabilities, security features, and security tests. (The DOC abbreviated certification methodology is available on the NIST Computer Security website, (<http://csrc.ncsl.nist.gov/secpubs/>)). Additionally, the Contractor shall conduct security testing for the management, operational, and technical security control measures and safeguards for RPS. The Contractor shall utilize the DOC Abbreviated Certification Methodology Worksheet 5 to document the security test results. The recommendations for mitigating identified system risks shall be categorized according to low, medium, or high. The Contractor shall then develop a *Security Test & Evaluation (ST&E) Report* for RPS. Note: NIST has recently developed draft revised guidance for conducting systems security certification and accreditation, (NIST Special Publication 800-37: Guidelines for the Security Certification and Accreditation of Federal Information Technology Systems, October 2002. This revised guidance has not yet been finalized, however the contractor should review the draft guidance and use it as a technical resource, to help assist in certification and accreditation planning.

### **2.2.5 Milestone 5: Update the IT Contingency Plan**

The Contractor shall develop a Draft *IT Contingency Plan* for RPS to be used on an interim basis

until contingency plan testing is completed. The IT Contingency Plan shall be prepared in accordance with NIST guidance, (Special Publication 800-34, June 2000, Contingency Planning Guide For Information Technology Systems).

Following the completion of contingency plan testing, the Contractor shall update the Draft *IT Contingency Plan* for RPS to include lessons learned from testing and shall submit a Final *IT Contingency Plan*.

#### **2.2.6 Milestone 6: Conduct IT Contingency Plan Training**

The Contractor shall develop *IT Contingency Plan Training* for RPS. The IT Contingency Plan training shall include the team members specific roles and responsibilities in the execution of the plan; a thorough understanding of the team checklists of procedures, including notification procedures; interdependencies of individual team checklists of procedures; and on-going evaluation of the effectiveness of the team checklists of procedures.

#### **2.2.7 Milestone 7: Conduct IT Contingency Plan Testing**

The Contractor shall conduct structured walk-through and checklist testing with identified key Agency personnel familiar with the RPS. Recommendations for improvements to the RPS IT Contingency Plan shall be made upon evaluation of the IT Contingency Plan test results and shall be incorporated into an *IT Contingency Plan Test Report* for RPS.

#### **2.2.8 Milestone 8: Develop the System Re-Certification and Re-Accreditation Report**

The Contractor shall develop a *System Certification Report* for RPS in accordance with the NRC Management Directive 12.5. The Contractor shall utilize the DOC Abbreviated Certification Methodology Worksheets 1-6 to document the system description, identified vulnerabilities, security features, security tests, security test results, and evaluation and recommendations and a certification statement for RPS. The NRC Office of NRR is the system owner and will sign the certification statement. The certification statement will be submitted to the NRC Senior IT Security Officer, who will review it and provide a recommendation for an approval to operate to the NRC Chief Information Officer, who is the Designated Approving Authority (DAA).

#### **2.2.9 Milestone 9: Complete the Security Self-Assessment (Appendix A) of the Self-Assessment Guide for Information Technology Systems (NIST Special Publication 800-26)**

The contractor shall complete the Security Self-Assessment (Appendix A) of the Self-Assessment Guide for Information Technology Systems (NIST Special Publication 800-26) for RPS. The contractor shall review the RPS *Risk Assessment Reports* and *System Security Plans*, other related documentation, and interview up to five (5) NRC employees to determine the status of each of the 17 control topic areas. The contractor shall also determine the status of each control by quantifying the level of maturity of the control in one of the following categories:

Level 1 - Control objective documented in a security policy

Level 2 - Security controls documented as procedures

Level 3 - Procedures have been implemented

Level 4 - Procedures and security controls are tested and reviewed

Level 5 - Procedures and security controls are fully integrated into a comprehensive program

The contractor shall use the General Accounting Office (GAO) Federal Information Systems Control Audit Methodology (FISCAM) as a guide when categorizing each of the controls into the appropriate maturity level. The contractor shall analyze the results of the self assessment and document action plans that management can then use to remediate all controls that are categorized below level 5.

#### **2.2.10 Milestone 10: Exit Briefing Presentation**

The Contractor shall develop an *Exit Briefing Presentation* with NRC staff. The presentation shall include a brief summary of the work performed and documents prepared, and answer NRC staff questions.

### **3.0 REPORTING REQUIREMENTS**

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

The contractor shall provide a Monthly Technical Progress Report to the Project 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 listing of the efforts completed during the period and milestones reached, or, if missed, an explanation provided;
- 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.

#### **3.3 Place of Reports Delivery**

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

- Louis Numkin: Project Officer (3 hard copies, and 3 CDs with all documents in WordPerfect or MS Word format)

### **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 ninety (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 ninety (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 MEETINGS AND DELIVERABLES**

### **KICK-OFF MEETING**

The contractor shall attend a kick-off meeting within five (5) business days after task award to introduce the NRC Project Officer and the Technical Project Officer. During this meeting, discussion shall include the ten (10) milestones and corresponding deliverables as identified in Section 2.0 - Scope of Work.

The Contractor shall deliver three (3) copies of all earlier specified deliverables to the NRC Project Officer during normal business hours. Final deliverables (except Monthly Progress 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 five (5) 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 office of the Project Officer. Based on the clients work schedule, this meeting can be held by phone at the request of the client.

## 6.0 PERIOD OF PERFORMANCE

The period of performance for this delivery order is from the date of award through December 31, 2004.

## 7.0 TRAVEL

None

## 8.0 2052.204-70 SECURITY (March 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 unclassified Safeguards Information, 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, proprietary data (trade secrets) or confidential or privileged technical, business, or financial information, including Commission plans, policies, reports, financial plans, other (Official Use Only) 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.

- (I) 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.

(End of Clause)

#### **9.0 Badge Requirements for Unescorted Building Access to NRC Facilities (February 2004)**

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. 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.

(End of Clause)

#### **10.0 SECURITY REQUIREMENTS FOR BUILDING ACCESS APPROVAL (February 2004)**

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 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 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 shall be required to complete and submit to the contractor representative an acceptable GSA Form 176 (Statement of Personal History), 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 GSA Form 176. 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.

#### **11.0 SECURITY REQUIREMENTS FOR INFORMATION TECHNOLOGY ACCESS APPROVAL (February 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."

(End of Clause)

#### **12.0 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.

### **13.0 PROJECT OFFICER AUTHORITY (February 2004)**

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

Name: Louis Numkin

Address: U. S. Nuclear Regulatory Commission

Mail Stop (T-6D2, Washington, D. C. 20555-0001

Telephone Number: 301-415-5906

(b) Performance of the work under this contract 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 (SOW) or changes to specific travel identified in the SOW), fills in details, or otherwise serves to accomplish the contractual SOW.

(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 contract, approval of technical reports, drawings, specifications, and technical information to be delivered by the contractor to the Government under the contract.

(c) Technical direction must be within the general statement of work stated in the contract. 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 contract.

(2) Constitutes a change as defined in the "Changes" clause of this contract.

(3) In any way causes an increase or decrease in the total estimated contract cost, the fixed fee, if any, or the time required for contract performance.

(4) Changes any of the expressed terms, conditions, or specifications of the contract.

(5) Terminates the contract, settles any claim or dispute arising under the contract, 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 contract accordingly. Upon receiving the notification from the contractor, the contracting officer shall issue an appropriate contract 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 contract.

(h) A failure of the parties to agree upon the nature of the instruction or direction or upon the contract 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 contract.

(4) Assist the contractor in obtaining the badges for the contractor personnel.

(5) Immediately notify the Security Branch, Division of Facilities and Security (SB/DFS) (via e-mail) when a contractor employee no longer requires access authorization and return of any NRC issued badge to SB/DFS within three days after their termination."

(6) Ensure that all contractor employees that require access to classified Restricted Data or National Security Information or matter, access to sensitive unclassified information (Safeguards, Official Use Only, and Proprietary information) access to sensitive IT systems or data, unescorted access to NRC controlled buildings/space, or unescorted access to protected and vital areas of nuclear power plants receive approval of SB/DFS prior to access in accordance with Management Directive and Handbook 12.3.

(End of Clause)

CONTINUATION PAGE

A.8 LIST OF ATTACHMENTS

ATTACHMENT  
NUMBER

TITLE

1 Billing Instructions

2 NRC Form 187 Contract Security and/or  
Classification Requirements

**BILLING INSTRUCTIONS FOR  
FIXED PRICE CONTRACTS (October 2003)(With Reimbursable Travel)**

**General:** The contractor is responsible during performance and through final payment of this contract for the accuracy and completeness of the data within the Central Contractor Registration (CCR) database, and for any liability resulting from the Government's reliance on inaccurate or incomplete CCR data. The contractor shall prepare vouchers or invoices as prescribed herein. **FAILURE TO SUBMIT VOUCHERS/INVOICES IN ACCORDANCE WITH THESE INSTRUCTIONS WILL RESULT IN REJECTION OF THE VOUCHER/INVOICES AS IMPROPER.**

**Form:** Claims shall be submitted on the payee's letterhead, voucher/invoices, or on the Government's Standard Form 1034, "Public Voucher for Purchases and Services Other than Personal," and Standard Form 1035, "Public Voucher for Purchases Other than Personal-Continuation Sheet." These forms are available from the U.S. Government Printing Office, 710 North Capitol Street, Washington, DC 20401.

**Number of Copies:** An original and three copies shall be submitted. 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 - T-7-I-2  
Washington, DC 20555-0001**

A copy of any invoice which includes a purchase of property valued at the time of purchase at \$5000 or more, shall additionally be sent to:

**NRC Property Management Officer  
Administrative Services Center  
Mail Stop -O-2G-112  
Washington, DC 20555-0001**

**HAND-DELIVERY OF VOUCHERS/INVOICES IS DISCOURAGED AND WILL NOT EXPEDITE PROCESSING BY THE NRC. However, should you choose to deliver vouchers/invoices by hand, including delivery by any express mail service or special delivery service which uses a courier or other person to deliver the vouchers/invoices 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 - Mail Room  
11555 Rockville Pike  
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.**

**Agency Payment Office:** Payment will continue to be made by the office designated in the contract in Block 12 of the Standard Form 26 or Block 25 of the Standard Form 33, whichever is applicable.

**Frequency:** The contractor shall submit a voucher or invoice only after the NRC's final acceptance of services rendered or products delivered in performance of the contract unless otherwise specified in the contract.

**Preparation and Itemization of the Voucher/Invoice:** The voucher/invoice shall be prepared in ink or by typewriter (without strike-overs). Corrections or erasures must be initialed. To be considered a proper voucher/invoice, all of the following elements must be included:

1. Contractor's Data Universal Number (DUNS) or DUNS+4 number that identifies the contractor's name and address. The DUNS+4 number is the DUNS number plus a 4-character suffix that may be assigned at the discretion of the contractor to identify alternative Electronic Funds Transfer (EFT) accounts for the same parent concern.
2. Contract number.
3. Sequential voucher/invoice number.
4. Date of voucher/invoice.
5. Payee's name and address. Show the name of the Payee as it appears in the contract and its correct address. If the Payee assigns the proceeds of this contract as provided for in the assignment of claims terms of this contract, the Payee shall require as a condition of any such assignment, that the assignee shall register separately in the Central Contractor Registration (CCR) database at <http://www.ccr.gov> and shall be paid by EFT in accordance with the terms of this contract. See Federal Acquisition Regulation 52.232-33(g) Payment by Electronic Funds Transfer - Central Contractor Registration (October 2003).
6. Description of articles or services, quantity, unit price, and total amount.
7. For contractor acquired property list each item purchased costing \$50,000 or more and having a life expectancy of more than 1 year and provide: (1) an item description, (2) manufacturer, (3) model number, (4) serial number, (5) acquisition cost, (6) date of purchase, and (7) a copy of the purchasing document.
8. Weight and zone of shipment, if shipped by parcel post.
9. Charges for freight or express shipments. Attach prepaid bill if shipped by freight or express.
10. Instructions to consignee to notify the Contracting Officer of receipt of shipment.
11. For Indefinite Delivery contracts or contracts under which progress payments are authorized, the final voucher/invoice shall be marked "FINAL VOUCHER" OR "FINAL INVOICE."

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

**Supersession:** These instructions supersede any previous billing instructions.

C:\WINDOWS\Profiles\dak1\Desktop\CISSCO SECURITY PROCUREMENTS\SECURITY  
PROCUREMENT\NRC-03-04-029 COMPUTER SECURITY REV -UPDATE OF THE NRR RPS  
SYSTEM\Billing Instruct FP 2003.wpd

## CONTRACT SECURITY AND/OR CLASSIFICATION REQUIREMENTS

**COMPLETE CLASSIFIED ITEMS BY SEPARATE CORRESPONDENCE**

1. CONTRACTOR NAME AND ADDRESS

To Be Determined

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

04/30/2004

C. PROJECTED COMPLETION DATE

09/30/2004

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

*COMPUTER SECURITY REVIEW /  
UPDATED to NRP/RPS SYSTEM*

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  <p style="text-align: center;"><b>Louis M Numkin</b> Senior Computer Security Specialist</p>	SIGNATURE 	DATE <p style="text-align: right;">5/13/04</p>
--	---	---

**7. CLASSIFICATION GUIDANCE**

NATURE OF CLASSIFIED GUIDANCE IDENTIFICATION OF CLASSIFICATION GUIDES

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

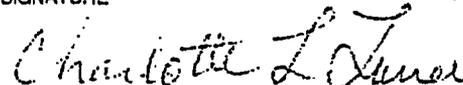
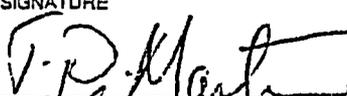
- AUTHORIZED CLASSIFIER (Name and Title)
  DIVISION OF FACILITIES AND SECURITY

**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  <b>Charlotte L. Turner, PMAS/OCIO</b>	SIGNATURE 	DATE <p style="text-align: right;">4/27/04</p>
B. DIRECTOR, DIVISION OF FACILITIES AND SECURITY  <b>Thomas O. Martin, DFS/ADM</b>	SIGNATURE 	DATE <p style="text-align: right;">4/30/04</p>
C. DIRECTOR, DIVISION OF CONTRACTS AND PROPERTY MANAGEMENT <small>(Not applicable to DOE agreements)</small> <b>KATHRYN J. REESE DCI/ADM</b>	SIGNATURE 	DATE <p style="text-align: right;">5/13/04</p>

REMARKS