

# ORDER FOR SUPPLIES OR SERVICES

PAGE OF PAGES  
1 3

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

1. DATE OF ORDER 05-16-2002		2. CONTRACT NO. (If any) GS-35F-0607J		6. SHIP TO:				
3. ORDER NO. NRC-33-01-192-001		MODIFICATION NO.		a. NAME OF CONSIGNEE U.S. Nuclear Regulatory Commission				
4. REQUISITION/REFERENCE NO. CIO-01-179-014		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		b. STREET ADDRESS ATTN: Louis Numkin Mail Stop: T-6F15		c. CITY Washington	d. STATE DC	e. ZIP CODE 20555
7. TO:				f. SHIP VIA				
a. NAME OF CONTRACTOR Corbett Technologies, Inc.				8. TYPE OF ORDER				
b. COMPANY NAME ATTN: Carl F. Vogt				<input type="checkbox"/> a. PURCHASE ORDER		<input checked="" type="checkbox"/> b. DELIVERY/TASK ORDER		
c. STREET ADDRESS 1600 Duke Street, Suite 600				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.		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.		
d. CITY Alexandria		e. STATE VA	f. ZIP CODE 22314					
9. ACCOUNTING AND APPROPRIATION DATA 31X0200 JCN: J2923 B&R: 22015101160 BOC: 252A OBLIGATE: \$51,740.80				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 BAL. NO.	15. DELIVER TO F.O.B. POINT ON OR BEFORE See Below		16. DISCOUNT TERMS N/A		
13. PLACE OF				FOR INFORMATION CALL: (No collect calls)				
a. INSPECTION		b. ACCEPTANCE						

**17. SCHEDULE (See reverse for Rejections)**

ITEM NO. (A)	SUPPLIES OR SERVICES (B)	QUANTITY ORDERED (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)	QUANTITY ACCEPTED (G)
	<p>The U.S. Nuclear Regulatory Commission (NRC) hereby accepts Corbett Technologies proposal dated 4/16/02, to provide services in accordance with the attached Statement of Work.</p> <p>The total firm fixed price for this delivery order is \$51,740.80.</p> <p>The Project Officer is Louis Numkin (301) 415-5906.</p>					

SEE BILLING INSTRUCTIONS ON REVERSE	18. SHIPPING POINT		19. GROSS SHIPPING WEIGHT		20. INVOICE NO.		\$51,740.80	SUBTOTAL	
	21. MAIL INVOICE TO:								17(h) TOTAL (Cont. pages)
	a. NAME U.S. Nuclear Regulatory Commission Division of Contracts & Property Mgmt.								
	b. STREET ADDRESS (or P.O. Box) ATTN: Mail Stop T-7-I2 Sharlene McCubbin, Contract Specialist								
c. CITY Washington			d. STATE DC	e. ZIP CODE 20555			\$51,740.80	17(i). GRAND TOTAL	

22. UNITED STATES OF AMERICA BY (Signature)  	23. NAME (Typed) Mark J. Flynn  TITLE: CONTRACTING/ORDERING OFFICER
--------------------------------------------------------	------------------------------------------------------------------------------



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

### **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)  
for the PC-Integrated Events (PIE) System**

**1.0 BACKGROUND**

The Contractor shall submit a **Firm Fixed Price** 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 required for the NRR PC-Integrated Events (PIE) System to ensure compliance with current Federal guidelines, which includes a Risk Assessment Report, a System Security Plan (SSP), a Security Test & Evaluation (ST&E) Plan, security controls testing, a ST&E Report, a Business Continuity Plan (BCP), and a System Certification Report.

**1.1 SYSTEM DESCRIPTION**

The Events Assessment, Generic Communications, and Non-Power Reactors Branch (REXB) within NRR/DRIP is specifically tasked with providing NRR, the EDO's office and the public at large (via FOIA's) with information relating to the history, patterns of occurrence, and research relating to event-related information. In order to perform this function REXB operates the Events Tracking System (ETS) and a number of sub-programs that are called within this program. These are the Events Notification System (also called Operations Officer Support System [OOSS]), the Preliminary Notification System (PN), and the Morning Report System (MR). Additionally, there are several hypertext retrieval systems that are being operated to enhance the ability to search for document types. Over the last decade, the REXB staff have primarily used the Folios Views, version 2.1 to accomplish this task. This system has been used to provide raw information, perform queries, and to correlate between regulatory documents and actual plant events. Zylmage for Windows for Inspection Reports is also used. All together, these systems are known as NRR PIE (or PC-LAN Integrated Events) System.

## 1.2 SYSTEM ENVIRONMENT

PIE was designed as a Novell-based server storage application to operate within the Agency local area network and wide area network (LAN/WAN) infrastructure established by NRC's Next Generation Network initiative. The desktop software resides on the standard personal computer (PC) desktop configuration, typically a networked Pentium II class machine with a 3.5" diskette drive and a CD drive, running under Windows NT Workstation 4.0.

## 1.3 SYSTEM INFORMATION SENSITIVITY AND CRITICALITY

**Confidentiality: Medium**

**Integrity: High**

**Availability: Medium**

## 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** 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: Develop a Risk Assessment Report
- Milestone 3: Develop a System Security Plan
- Milestone 4: Develop a Security Test & Evaluation (ST&E) Plan and Report
- Milestone 5: Develop a Business Continuity Plan
- Milestone 6: Develop a System Certification Report
- Milestone 7: 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*.

### **2.2.2 Milestone 2: Develop a Risk Assessment Report**

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 PIE System. Based on the results and analysis of interviews and data collection efforts, the Contractor shall conduct a risk assessment of the PIE operating environment, and develop a *Risk Assessment Report* for the PIE System.

The objectives of this risk assessment for the PIE System 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*.

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

Based on the results and analysis of interviews and data collection efforts, the Contractor shall develop the *System Security Plan*. 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*.

### **2.2.4 Milestone 4: Develop the Security Test & Evaluation (ST&E) Test Plan and Report**

The Contractor shall develop a *Security Test & Evaluation (ST&E) Test Plan* 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*. This milestone is divided into two (2) subtasks.

#### **2.2.4.1 Milestone 4-1: 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 PIE System 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*.

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

The Contractor shall conduct system testing of safeguards for the PIE System and provide recommendations for improvements to the system using the *System Security Plan* developed in Milestone 3 and the *System Test & Evaluation (ST&E) Test Plan* developed in Milestone 4-1. Recommendations for improvements to the PIE System 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.

**Medium Priority:** Though important to enhancing the security of the system, corrective action of *Medium 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 PIE 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*.

#### 2.2.5 Milestone 5: Develop a Business Continuity Plan

The Contractor shall develop a *Business Continuity Plan* 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 PIE System; 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 PIE System business continuity information within the NRC's LDRPS application.

The Contractor shall develop a Draft and Final *Business Continuity Plan*.

## 2.2.6 Milestone 6: Develop the System Certification Report

The Contractor shall develop a *System Certification Report* 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 PIE System.

The *System Certification Report* shall include the 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*.

## 2.3 Schedule of Deliverables

Deliverable #	Milestone #	Deliverable Title	T+# Due Date
1	1	Draft Project Management Plan	T + 2
2	1	Final Project Management Plan	T +4 (at Kick Off)
3	2	Draft Risk Assessment Report	
4	2	Final Risk Assessment Report	T + 15
5	3	Draft System Security Plan	
6	3	Final System Security Plan	T + 32 *
7	4-1	Security Test & Evaluation (ST&E) Plan	
8	4-2	Security Test & Evaluation (ST&E) Report	T + 25
9	5	Draft Business Continuity Plan	
10	5	Final Business Continuity Plan	T + 53
11	6	System Certification Report	T + 67
12	7	Exit Briefing Presentation	T + 74

\* This Statement of Work requires that the *System Security Plan* be completed not later than 14 June 2002.

**2.3.1 SCHEDULE OF PAYMENTS**

The contractor shall receive two payments as follows under the subject delivery order.

The contractor shall receive the first payment in the amount of \$24,663.04 at the completion of the following deliverables:

1.	Project Management	\$ 3,082.88
2.	Risk Assessment	\$10,019.36
3.	System Security Plan	\$11,560.80
	<b>Total Amount</b>	<b>\$24,663.04</b>

The contractor shall receive the second payment in the amount 27,077.76 at the completion of the following deliverables:

4.	Security Test & Evaluation	\$10,212.04
5.	Business Continuity Plan	\$ 7,707.20
6.	Certification Report	\$ 3,853.60
7.	Exit Brief	\$ 1,734.12
8.	QA/Admin and ODC	\$ 3,570.80
	<b>Total Amount</b>	<b>\$27,077.76</b>

The Total Fixed Price is ..... **\$51,740.80**

**3.0 REPORTING REQUIREMENTS**

**3.1 Bi-Weekly Technical Progress Reports**

The contractor shall provide a bi-weekly Technical Progress Report to the Project Officer. The report is due the Wednesday of every other week from project initiation 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:

- Name: Louis Numkin, Project Officer (3 copies)
- Address: US Nuclear Regulatory Commission  
OCIO/ADD/CSS  
ms: T-6-F-15  
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 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 MILESTONES AND DELIVERABLES

The Contractor shall conduct an orientation meeting no later than five (5) days from the date of the task award. During this meeting, discussion shall include the seven (7) 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 Project Officer 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 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 August 30, 2002.

## **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 thirty [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:

1. 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.
2. The contractor agrees to conform to all security regulations and requirements of the Commission including but not limited to an auditable drug-testing program for all contracted personnel.

(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 (PERSEC), Division of Facilities and Security (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 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 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 NRC Management Directive 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 NRC Management Directive 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 NRC Management Directive 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 NRC Management Directive 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 thirty [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 NRC Management Directive 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 NRC Management Directive 12.3, Part I. The individual will be subject to a reinvestigation every ten (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 NRC Management Directive 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 NRC Management Directive 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 NRC Management Directive 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 thirty [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

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.

(b) 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.

(c) 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.

(d) The contractor shall proceed promptly with the performance of technical directions duly issued by the project officer in the manner prescribed by this clause and within the project officer's authority under the provisions of this clause.

(e) If, in the opinion of the contractor, any instruction or direction issued by the project officer is within one of the categories as defined in paragraph (c) of this section, the contractor may not proceed but shall notify the contracting officer in writing within five (5) working days after the receipt of any instruction or direction and shall request the contracting officer to modify the order accordingly. Upon receiving the notification from the contractor, the contracting officer shall issue an appropriate modification or advise the contractor in writing that, in the contracting officer's opinion, the technical direction is within the scope of this article and does not constitute a change under the "Changes" clause.

(f) Any unauthorized commitment or direction issued by the project officer may result in an unnecessary delay in the contractor's performance and may even result in the contractor expending funds for unallowable costs under the order.

(g) A failure of the parties to agree upon the nature of the instruction or direction or upon the order action to be taken with respect thereto is subject to 52.233-1 - Disputes.

(h) In addition to providing technical direction as defined in paragraph (b) of the section, the project officer shall:

- (1) Monitor the contractor's technical progress, including surveillance and assessment of performance, and recommend to the contracting officer changes in requirements.
- (2) Assist the contractor in the resolution of technical problems encountered during performance.
- (3) Review all costs requested for reimbursement by the contractor and submit to the contracting officer recommendations for approval, disapproval, or suspension of payment for supplies and services required under this order.
- (4) Assist the contractor in obtaining the badges for the contractor personnel.
- (5) Immediately notify PERSEC/DFS (via e-mail) when a contractor employee no longer requires access authorization and return the individuals badge to PERSEC/DFS within three days after their termination.

## **10.0 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.

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

- The Insider Threat To U.S. Government Information Systems, NSTISSAM INFOSEC/ 1-99, July 1999.
- 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.
- NRC OCIO System Development and Life Cycle Management (SDLCM) Methodology, Version 1.2, January 31, 2001.
- Independent Evaluation of the Nuclear Regulatory Commission Information Security Program, Required by the Government Information Reform Act, August 29, 2001.

## **11.0 KICK-OFF MEETING**

A kick-off meeting will be held within five (5) business days after task award to introduce the NRC Project Officer and the Technical Project Officer.