

ORDER FOR SUPPLIES OR SERVICES

PAGE OF PAGES
1 4

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

1. DATE OF ORDER 09-27-2001		2. CONTRACT NO. (If any) GS-35F-0079J		6. SHIP TO:	
3. ORDER NO. NRC-33-01-191-001		MODIFICATION NO.		4. REQUISITION/REFERENCE NO. CI0-01-179-006	
5. ISSUING OFFICE (Address correspondence to) U.S. Nuclear Regulatory Commission Division of Contracts and Property Mgt. Attn: T-7-I-2 IT Acquisition Management Branch Washington DC 20555				a. NAME OF CONSIGNEE U.S. Nuclear Regulatory Commission	
				b. STREET ADDRESS ATTN: Louis Grosman Mail Stop: T-6F15	
				c. CITY Washington	e. ZIP CODE 20555
				d. STATE DC	
7. TO:				f. SHIP VIA	
a. NAME OF CONTRACTOR Allied Technology				8. TYPE OF ORDER	
b. COMPANY NAME ATTN: William P. Conner 1803 Research Boulevard				<input type="checkbox"/> a. PURCHASE ORDER <input checked="" type="checkbox"/> b. DELIVERY/TASK ORDER	
c. STREET ADDRESS Suite 601				Reference your Please furnish the following on the terms and conditions specified on both sides of this order and on the attached sheet, if any, including delivery as indicated.	
d. CITY Rockville		e. STATE MD		f. ZIP CODE 20850	
9. ACCOUNTING AND APPROPRIATION DATA 31X0200.110 JCN: 1100 B&R: 11015521115 BOC: 252A OBLIGATE: \$53,129.84				10. REQUISITIONING OFFICE CIO OCIO/PRMD	
11. BUSINESS CLASSIFICATION (Check appropriate box(es))					
<input checked="" type="checkbox"/> a. SMALL <input type="checkbox"/> b. OTHER THAN SMALL <input checked="" type="checkbox"/> c. DISADVANTAGED <input type="checkbox"/> d. WOMEN-OWNED					
12. F.O.B. POINT Destination		14. GOVERNMENT B/L NO.		15. DELIVER TO F.O.B. POINT ON OR BEFORE See Below	
				16. DISCOUNT TERMS N/A	
13. PLACE OF		FOR INFORMATION CALL: (No collect calls)			
a. INSPECTION		b. ACCEPTANCE			

17. SCHEDULE (See reverse for Rejections)

See CONTINUATION Page

ITEM NO. (A)	SUPPLIES OR SERVICES (B)	QUANTITY ORDERED (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)	QUANTITY ACCEPTED (G)
	The U.S. Nuclear Regulatory Commission (NRC) hereby accepts Allied's proposal dated 9/13/01 and amended on 9/24/01, which is hereby incorporated by reference and made a part of this order. The labor categories are as follows:					
	Senior Management Analyst/PM	104	Hours	117.28	\$12,197.12	
	Senior Consultant	152	Hours	117.28	\$17,826.56	
	Senior Systems Analyst	64	Hours	78.19	\$5,004.16	
	Lead ADP Scientist	104	Hours	78.19	\$8,131.76	
	Security Systems Specialist	104	Hours	73.31	\$7,624.24	
	Computer Security Systems Specialist	40	Hours	58.65	\$2,346.00	
	The ceiling amount of this Labor Hour contract is \$53,130.					
	The level hours are estimated, and may be increased from time to time by the Contracting Officer by written modification.					
	The obligated amount is \$53,130. The obligated amount shall, at no time, exceed the ceiling. When and if the					

SEE BILLING INSTRUCTIONS ON REVERSE	18. SHIPPING POINT		19. GROSS SHIPPING WEIGHT		20. INVOICE NO.		\$53,129.84	SUBTOTAL
	21. MAIL INVOICE TO:							17(h) TOTAL (Cont. pages)
	a. NAME U.S. Nuclear Regulatory Commission Division of Contracts & Property Mgmt.							17(i). GRAND TOTAL
	b. STREET ADDRESS (or P.O. Box) ATTN: Mail Stop T-7-I2							
c. CITY Washington		d. STATE DC	e. ZIP CODE 20555				\$53,129.84	

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

OPTIONAL FORM 347 (6/95)

TEMPLATE-ADM1001

ADM02

ORDER FOR SUPPLIES OR SERVICES SCHEDULE - CONTINUATION

PAGE NO.

2

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

DATE OF ORDER 09-27-2001		CONTRACT NO. GS-35F-0079J		ORDER NO. NRC-33-01-191-001		
ITEM NO. (A)	SUPPLIES OR SERVICES (B)	QUANTITY ORDERED (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)	QUANTITY ACCEPTED (G)
	<p>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 order. Any work undertaken by the Contractor in excess of the obligated amount specified above is done so at the Contractor's sole risk.</p> <p>FAR Clause 52.232-7 is applicable to this order.</p> <p>The period of performance is estimated from date of award through March 31, 2002.</p> <p>The Project Officer is Louis Grosman, (301) 415-5826.</p> <p>ATTACHMENTS:</p> <p>Statement of Work Billing Instructions ACH Vendor Information Form</p>					
TOTAL CARRIED FORWARD TO 1ST PAGE (ITEM 17(H))						

SUPPLEMENTAL INVOICING INFORMATION

If desired, this order (or copy thereof) may be used by the Contractor as the Contractor's invoice, instead of a separate invoice, provided the following statement, (signed and dated) is on (or attached to) the order: "Payment is requested in the amount of \$_____. No other invoice will be submitted." However, if the Contractor wishes to submit an invoice, the following information must be provided: contract number (if any), order number, item number(s), description of supplies or services, sizes, quantities, unit prices, and extended totals. Prepaid shipping costs will be indicated as a separate item on the invoice. Where shipping costs exceed \$10 (except for parcel post), the billing must be supported by a bill of lading or receipt. When several orders are invoiced to an ordering activity during the same billing period, consolidated periodic billings are encouraged.

RECEIVING REPORT

Quantity in the "Quantity Accepted" column on the face of this order has been: ☐ inspected, ☐ accepted, ☐ received by me and conforms to contract. Items listed below have been rejected for the reasons indicated.

SHIPMENT NUMBER		PARTIAL	DATE RECEIVED	SIGNATURE OF AUTHORIZED U.S. GOV'T REP.	DATE
		FINAL			
TOTAL CONTAINERS		GROSS WEIGHT	RECEIVED AT	TITLE	

	REPORT OF REJECTIONS
--	-----------------------------

[illegible]

TASK ORDER TERMS AND CONDITIONS

NOT SPECIFIED IN THE CONTRACT

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

2052.209-72

CONTRACTOR ORGANIZATIONAL CONFLICTS OF INTEREST JAN 1993

A.2 ELECTRONIC PAYMENT

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

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

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

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

A.3 SEAT BELTS

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

Technical Requirements
To Provide Computer Security Services
For The
United States Nuclear Regulatory Commission (NRC)
Office of Chief Information Officer (OCIO)
For the Conduct of an
Internal Threat Vulnerability Assessment

Technical Requirements To Provide Computer Security Services For The Office of Chief Information Officer (OCIO)

1. General

1.1_ Background

Insiders pose the greatest security threat, but detect infrastructures primarily focus on outsiders. Most enterprises, such as the NRC, are under invested in techniques and processes to detect malicious insider activity. The insider threat arises from multiple sources. There is the threat posed by disgruntled employees or contractors, especially those who are to be terminated for cause. There is also the threat posed by users of the system who negligently or inadvertently fail to follow security requirements for the handling and labeling of system output or media, or the rules against the introduction of software or data imported from unauthorized sources. There is the threat of the co-option of users with authorized access to the system, contractor support personnel, or NRC employees or other NRC contract personnel with physical access to the system components arising from the motivation of financial gain. Finally, there is the threat arising from the failure of authorized users to employ proper procedures for the entry or manipulation of system data arising from negligence or the failure to properly train users in the use and operation of the system. Of these, disgruntled or co-opted systems administration personnel who have the ability to alter or bypass most, if not all, of the system's technical protection mechanisms could mount the most serious of all types of possible attacks against the system.

These insider threats can be manifested in the following ways:

- Execution of denial-of-service attacks
- Introduction into the system of viruses, worms, or other malicious software
- Destruction or corruption of data, software, or hardware (intentional or unintentional)
- Exposure of sensitive data to compromise through the improper labeling or handling of printed output or magnetic media
- Unauthorized reading, copying, or disclosure of sensitive information

1.2 Mission

The mission of NRC is to ensure adequate protection for the public health and safety, the common defense and security, and the environment in the use of nuclear materials in the United States. The responsibility of the NRC includes regulation of commercial nuclear power plants; research, test, and training reactors; fuel cycle facilities; medical, academic, and industrial uses of nuclear materials; and the transport, storage, and disposal of nuclear materials and wastes. The NRC performs its mission by setting standards and requirements in the form of rules, license conditions, and regulatory guidance, that licensees must meet to design, construct, and operate safe facilities; inspecting facilities and taking enforcement action, as necessary, to ensure that such standards are followed; and conducting research to support, assess, or refine judgements used in regulatory decisions.

The Nuclear Regulatory Commission's (NRC) Office of the Chief Information Officer (OCIO) mission includes the safeguarding of Information Technology (IT) assets from unauthorized access and use ensuring the highest degree of information assurance. Areas of interest include network and system security assessments, penetration analysis, internal controls, and security products (e.g., firewalls).

In accordance with the Office of Management and Budget (OMB) Circular A-130, Appendix III, the NRC is required to perform risk assessments, develop security plans, prepare contingency plans, provide contingency plan training to personnel, test contingency plans, and test security features, where applicable, for its sensitive systems.

The NRC requires the support of a Contractor to perform a Risk Assessment of potential Entity Wide Internal Threats by reviewing its internal information technology security controls, posture, and to ensure effective management control of computer rights and privileges are in place vis-à-vis the "insider threat," to identify security weaknesses and vulnerabilities, and to provide recommendations to improve information technology security controls, policies, procedures, and technology to better counter this threat within the NRC. The contractor must ensure that the work conforms with all Federal Requirements and NRC Management Directives. NRC has offices at five locations in the United States: Headquarters located in Rockville, Maryland; and Regions 1 through 4 located respectively in King of Prussia, Pennsylvania; Atlanta, Georgia; Lisle, Illinois, and Arlington, Texas. In addition, NRC has several separate field offices, plus NRC Resident Inspectors located at each licensed commercial power reactor site.

2.0 Planned Solutions

2.1 Plans for Performance

The Contractor shall propose to complete this project in four (4) milestones and corresponding deliverables, on a Time and Materials (T&M) basis. Each milestone consists of performing required tasks, as specified in this Statement of Work (SOW), resulting in specific deliverables, as described below.

- Milestone 1: Develop and Deliver a Draft and Final Project Work Plan and Approach for the Internal Threat Vulnerability Project
- Milestone 2: Perform Internal Threat Vulnerability Assessment
- Milestone 3: Develop and Deliver a Draft and a Final Vulnerability, Threat, and Risk Assessment Report
- Milestone 4: Exit Briefing Presentation

The Contractor shall perform all necessary support activities in a phased approach to ensure NRC an economy of scale in level of effort and cost-savings. The Contractor shall re-utilize developed techniques to conduct the insider threat vulnerability assessment and to produce the Internal Threat Final report. The Contractor shall ensure that specifics pertaining to the NRC are fully addressed and that final deliverables can "stand alone" serving as independent documents.

2.2 Technical Approach

Milestone 1: Project Work Plan

The Contractor shall prepare and deliver a draft and final Project Work Plan that details project milestones, deliverables, schedules, management processes, and approach. During this milestone, the Contractor shall perform an extensive review of published documentation on the subject of the *Insider Threat* and other pertinent security related best practices, mandates and guidelines that apply to all Federal agencies. These documents may include:

- Title VIII - Acquisition Policy, Acquisition Management, and Related Matters, Subtitle G- Government Information Security Reform (GISRA), Subchapter II - Information Security
- The Insider Threat To U.S. Government Information Systems, NSTISSAM INFOSEC/1-99, July 1999
- National Institute of Standards and Technology (NIST) Special Publication 800-18, *Guide for Developing Security Plans for Information Technology Systems*;
- Office of Management and Budget (OMB) Circular A-130, Appendix III;
- Computer Security Act of 1987;

- Federal Information Processing Standard (FIPS) 102;
- NIST Special Publication 500-109;
- Federal statutes and regulations; and
- NRC directives.

Based on this review, the Contractor shall formulate issues and questions for necessary interview sessions, and shall develop a detailed Plan of Action and Milestones for performing the overall task that shall be contained in a *Project Work Plan* for performing the overall task.

The Contractor shall develop a Draft and Final *Project Work Plan* for the NRC as prescribed deliverables. The *Project Work Plan* is a presentation of the specific procedures and methodologies to be used in performing the security review, organizations affected, individuals to be interviewed, and a proposed schedule of milestones and deliverables. The *Project Work Plan* shall include project schedules, a deliverable schedule with dates, milestone objectives, and a management plan. The *Project Work Plan* for the NRC shall be presented to NRC personnel on a date coordinated with the OCIO Project Manager.

Milestone 2: Conduct Internal Threat Vulnerability Assessment

The Contractor shall perform an Internal Threats Vulnerability Assessment of the Agency to identify vulnerabilities and assess threats that result from NRC engineering design, configuration, operation, components, policies, procedures, inadequate control of computer rights and privileges, and staff activities; to identify potential undesirable or unauthorized events; to identify risks that could have a negative impact on the integrity, confidentiality, or availability of information processed or stored by, or transmitted through the NRC; to identify potential controls to reduce or eliminate the impact of risk events; and to establish responsibilities and milestones for the implementation of mitigating controls.

The objectives of this *Vulnerability Assessment* for the agency 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.

Internal threats that should be specifically be addressed should include:

Intentional Threats:

- Malicious attacks on NRC systems/data
- Running private business information on NRC systems
- Release of virus
- Interruption of computer operations
- Interruption of business continuity activities
- Unauthorized use of NRC data

Unintentional Threats:

- Disruption of NRC systems/data
- Virus passed along from software
- Use of personal software (i.e., games)

Other Threats:

- The extensive use of IT contractors by OCIO and other NRC organizations
- Separation of duties
- Foreign assignees and their access to systems and data

During this milestone, the Contractor shall perform data collection and interviews in accordance with the *Project Work Plan* prepared and approved in Milestone 1. Approximately ten to fifteen detailed interviews are anticipated with NRC employees and Contractor personnel located in the NRC White Flint complex.

During this milestone, the Contractor shall coordinate with OCIO Project Management to schedule potential interviews with identified key agency personnel familiar with the management, operations, and security of the agency and its related systems. The Contractor shall utilize this information to enhance, revise and update the results of the Vulnerability Assessment. The Contractor shall determine the risk for each NRC vulnerability and/or threat. The Contractor shall assess the impact to the NRC for identified vulnerabilities and the probability of threat exploitation success. The Contractor shall evaluate the potential operational and/or functionality damage that could occur to NRC or supporting architecture (hardware, software or personnel) or to systems with identified dependencies that could occur from a vulnerability and/or threat being exploited. 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 integrity, confidentiality, or availability of an asset); the level of concern (i.e., high, medium, or low); the associated controls; and the action(s) required to minimize each risk.

The Contractor shall incorporate the results of this process and develop and deliver both a Draft and Final *Risk Assessment Report* for the NRC as described above.

Milestone 3: Develop Vulnerability, Threat, and Risk Assessment Report

Based on the results and analysis of interviews and data collection efforts, and the *Internal Threat Vulnerability Assessment* findings obtained during Milestone 2, the Contractor shall deliver, as an output from Milestone 2, a draft and a final "NRC Vulnerability, Threat, and Risk Assessment Report" documenting the findings of each vulnerability, threat and/or risk. This comprehensive report shall document specific NRC vulnerabilities and threats and evaluate the risk represented by each. The report shall provide recommendations to mitigate the adverse impact of the identified vulnerabilities, threats, and risks. This report should include best practices; recommendations for improving operational methods for monitoring insider activities; a preliminary estimation of the status of necessary safeguards (i.e., in place, not in place, planned, or not applicable; the identification of new and/or emerging technologies that offer opportunities for improvement; and summarizes legal restrictions and issues.

Milestone 4: Exit Briefing Presentation

The Contractor shall conduct an *Exit Briefing Presentation* with NRC staff personnel which shall consist of an agenda sheet identifying the task, project, contractor, and document titles, as well as briefing slides used for the presentation. The presentation shall include a brief summary of the work performed and documents prepared, and answer NRC staff questions. This presentation shall include the identification of vulnerabilities, threat assessment, risk analysis, and recommendations for managing and reducing risk.

2.3 Constraints/Problem Areas

Any testing performed during this task which could cause systems or processes to be placed out of service for any length of time must be coordinated in advance with NRC.

No other constraints or problem areas are identified at this time. No hard-to-fill or difficult-to-hire issues are anticipated. Any constraints/problem areas identified during the progress of the project shall be documented in the detailed status reports and discussed with the OCIO Project Manager.

The Contractor shall submit a detailed status report by the fifth (5th) working day of each month. The report will clearly state the progress during the month, problems encountered that may delay successful completion of a task, planned activities for the succeeding month, and the estimated completion dates of all significant milestones, tasks, and/or deliverables.

3.0 Task Requirements and Other Information

In preparing the proposal, the Contractor should assume the following:

- Appropriately cleared Contractor analyst(s) shall be allowed access to appropriate areas and facilities housing NRC resources and assets during normal business hours.
- Task and deliverable schedules shall be finalized upon award of this task support contract and provided to the NRC technical point-of-contact.
- NRC shall have ten (10) workdays to review Drafts deliverables and five (5) workdays to review Final deliverables, and shall accept or reject the deliverable in writing. When NRC fails to complete the review within this review period, the deliverable shall become acceptable on an interim basis for payment only.
- Workspace, telephone, and limited reproduction support shall be provided for Contractor staff during on-site data collection periods. The NRC shall provide space for on-site conferences/meetings with NRC personnel related to this task. Requests for space must be made by the Contractor within three (3) working days prior to the scheduled meeting.

4.0 Schedule for Deliverables

The contractor shall provide the NRC Project Manager with a project management plan that includes a detailed staffing plan and schedule showing how the contractor and NRC resources will be expended to meet the project requirements. Each deliverable shall first be submitted in draft for NRC review. NRC shall have 5 working days to review each draft deliverable and respond with comments or approval. Upon approval by NRC of the original draft or the corrected draft, the deliverable shall be delivered in final form to the NRC Project Manager and NRC Contracting Officer. For each deliverable (draft or final), the Contractor shall provide one (1) hard copy and one (1) electronic version of the deliverable to the NRC Task Manager, unless otherwise indicated. All deliverables shall be formatted and prepared using Word Perfect 6/7/8 software products. If the Contractor utilizes other software for the preparation of these plans and reports, the Contractor shall bear the responsibility for converting the documents to Word Perfect readable products.

4.1 Kick-Off Meeting

A Kick-Off meeting will be held to introduce the NRC Project Manager for the project. At that time the contractor will provide a Project Management Plan which will include a detailed staffing plan and schedule showing how contractor and NRC resources will be expended to meet project requirements.

4.2 Monthly Progress Reports

The Contractor shall provide the NRC Project Manager (PM)/COTR and NRC Contracting Officer with a written monthly progress report. These are due to the NRC by the last workday at the end of each calendar month throughout the project's duration. The NRC PM/COTR shall be responsible for providing the monthly progress report to the Contracting Officer.

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 encountered or still outstanding with an explanation of the cause and resolution of the problem or how the problem will be resolved.

4.3 Monthly Financial Status Report

Monthly Financial Status Report

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

(a) Provide total estimated cost (value) of the project as reflected in the delivery order, the amount of funds available in the delivery order to date, and the balance of funds required to complete the work as follows:

Total estimated delivery order amount.

Total funds obligated to date.

Total costs incurred this reporting period.

Total costs incurred to date.

Provide a detail of all direct and indirect costs incurred during the reporting period for the entire delivery order, if applicable.

Balance of obligations remaining.

Balance of funds required to complete the delivery order.

Contractor Spending Plan (CSP) Status:

(b) Projected percentage of completion cumulative through the report period for the project as reflected in the current CSP.

Indicate if there has been a significant change in the original CSP projection in either dollars or percentage of completion. Identify the change, the reasons for the change, whether there is any projected overrun, and when additional funds would be required. If there have been no changes to the original NRC-approved CSP projections, a written statement to that effect is sufficient in lieu of submitting a detailed response to Item 8.

A revised CSP is required with the Financial Status Report whenever the contractor or the Contracting Officer has reason to believe that the total cost for performance of this delivery order will be either greater or substantially less than what had been previously estimated.

(c) If the data in this report indicates a need for additional funding beyond that already obligated, this information may only be used as support to the official report for funding required in accordance with the Limitation of Cost (LOC) Clause (FAR 52.232-20) or the Limitation of Funds (LOF) Clause (FAR 52.232-22), both of which are hereby incorporated by reference and made a part of this delivery order.

4.4 Table of Deliverables and Schedule of Delivery

Deliverables and due dates are summarized in the table below. Deliverable due dates are based on workdays.

The kick-off meeting shall be held no later than five (5) days from the date of the task award. During this meeting, discussion shall include the four (4) milestones and deliverables as identified in Exhibit 4-1, Schedule of Deliverables, that follows.

Item No.	DELIVERABLE DESCRIPTION	DATE DUE
1	Kick-Off Meeting	5 workdays after award or earlier
2	Monthly Progress Reports	Monthly
3	Deliver Project Management Plan	At Kick-off meeting
4	Deliver Draft Project Work Plan	10 workdays after award or earlier
5	Deliver Final Project Work Plan	15 workdays after award or earlier
6	Deliver Briefing to NRC staff on Project Work Plan	15 workdays after award or earlier
7	Deliver Draft Vulnerability, Threat, and Risk Assessment Report	40 workdays after award or earlier
8	Deliver Final Vulnerability, Threat, and Risk Assessment Report	50 workdays after award or earlier
9	Deliver Briefing to NRC Management	Date to be determined

Exhibit 4-1: Schedule of Deliverables

4.4 Instructions for Deliverables

Deliverables shall be delivered on the dates specified in the cost proposal and consistent with the deliverables schedules as shown in this statement of work. Each deliverable shall first be submitted in a draft for agency review. If the agency makes extensive changes to the first draft, the Contractor shall submit a corrected draft for agency review. Upon approval by agency of the draft, the deliverable shall be submitted in final form.

All written deliverables shall be phrased in language that can be understood by the non-technical layperson. Statistical and other technical terms used in the deliverable shall be defined in a glossary.

The agency shall have 5 working days to review draft deliverables upon receipt of delivery to the agency.

If for any reason a deliverable cannot be delivered within the scheduled time frame, the Contractor shall notify the Agency Project Manager or On-Site COTR in writing with cause of delay and the proposed revised schedule. This notice shall include the impact on the overall project. The Agency Project Manager or On-Site COTR shall make a business decision about the impact of the delay and forward the impact to the Contracting Officer with a courtesy copy provided to the NRC COTR.

All deliverables, in both draft and final form, shall be submitted as one electronic copy and one hard copy. The format for the deliverables is not specified except that it shall be consistent throughout the suite.

4.5 Place of Delivery-Reports

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

- (a) Name: Louis Grosman, Project Officer (2 copies)
Address: OCIO/ADD Mail Stop T6-F15
Washington, DC 20555
- Name: Mark Flynn, Contracting Officer (1 copy)
Address: ADM/DCPM/ITAMB Mail Stop T7-I2

5.0 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.

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

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

6.0 52.242-15 Stop Work Order

(a) The Contracting Officer may, at any time, by written order to the contractor, require the contractor to stop all, or any part, of the work called for by this delivery order for a period of 90 days after the order is delivered to the contractor, and for any further period to which the parties may agree. The order shall be specifically identified as a stop-work order issued under this clause.

Upon receipt of the order, the contractor shall immediately comply with its terms and take all reasonable steps to minimize the incurrence of costs allocable to the work covered by the order during the period of work stoppage. Within a period of 90 days after a stop-work order is delivered to the contractor, or within any extension of that period to which the parties shall have agreed, the Contracting Officer shall either - (1) Cancel the stop-work order; or (2) Terminate the work covered by the order as provided in the Default, or the Termination for Convenience of the Government, clause of this delivery order.

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

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

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

7.0 Period Of Performance

The period of performance for this delivery order is from the date of award through March 31, 2002.

8.0 Security

(a) Security/Classification Requirements Form. The attached NRC Form 187 (Attachment 1) furnishes the basis for providing security and classification requirements to prime contractors, subcontractors, or others (e.g., bidders) who have or may have an NRC contractual relationship that requires access to classified information or matter, access on a continuing basis (in excess of 30 or more days) to NRC Headquarters controlled buildings, or otherwise requires NRC photo identification or card-key badges.

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

(c) In connection with the performance of the work under this contract, the contractor may be furnished, or may develop or acquire, proprietary data (trade secrets) or confidential or privileged technical, business, or financial information, including Commission plans, policies, reports, financial plans, internal data protected by the Privacy Act of 1974 (Pub. L. 93-579), or other information which has not been released to the public or has been determined by the Commission to be otherwise exempt from disclosure to the public. The contractor agrees to hold the information in confidence and not to directly or indirectly duplicate, disseminate, or disclose the information in whole or in part to any other person or organization except as may be necessary to perform the work under this contract. The contractor agrees to return the information to the Commission or otherwise dispose of it at the direction of the contracting officer. Failure to comply with this clause is grounds for termination of this contract.

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

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

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

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

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

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

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

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

SITE ACCESS BADGE REQUIREMENTS

During the life of this contract, the rights of ingress and egress for contractor personnel must be made available, as required, provided that a badge is issued after favorable adjudication from the Personnel Security Branch, Division of Facilities and Security (PERSEC/DFS). In this regard, all contractor personnel whose duties under this delivery order require their presence on-site shall be clearly identifiable by a distinctive badge furnished by the Government. The Project Officer shall assist the contractor in obtaining the badges for the contractor personnel. It is the sole responsibility of the contractor to ensure that each employee has a proper Government-issued identification/badge at all times. All prescribed identification must be immediately (no later than three days) delivered to PERSEC/DFS for cancellation or disposition upon the termination of employment of any contractor personnel. Contractor personnel must have this identification in their possession during on-site performance under this contract. It is the contractor's duty to assure that contractor personnel enter only those work areas necessary for performance of delivery order work, and to assure the safeguarding of any Government records or data that contractor personnel may come into contact with.

SECURITY REQUIREMENTS FOR INFORMATION TECHNOLOGY SERVICES

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

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

CONTRACTOR SECURITY REQUIREMENTS FOR LEVEL I

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

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

A contractor employee shall not have access to NRC facilities, sensitive information technology systems or data until he/she is approved by Personnel Security Branch, Division of Facilities and Security (PERSEC/DFS) first for temporary access (based on a favorable adjudication of their security forms and checks) and final access (based on a favorably adjudicated LBI) in accordance with the procedures found in NRC MD 12.3, Part I. The individual will be subject to a reinvestigation every 10 years. **Timely receipt of properly completed security applications is a delivery order requirement. Failure of the contractor to comply with this condition within the ten work-day period may be a basis to void the notice of selection.** In that event, the Government may select another firm for award.

The contractor shall submit a completed security forms packet, including the SF-86, "Questionnaire for National Security Positions," and fingerprint charts, through the Project Officer to PERSEC/DFS for review and favorable adjudication, prior to the individual performing work under this contract. The contractor shall assure that all forms are accurate, complete, and legible (except for Part 2 of the questionnaire, which is required to be completed in private and submitted by the individual to the contractor in a sealed envelope), as set forth in MD 12.3 which is incorporated into this delivery order by reference as though fully set forth herein. Based on PERSEC review of the applicant's security forms and/or the receipt of adverse information by NRC, the individual may be denied access to NRC facilities, sensitive information technology systems or data until a final determination is made of his/her eligibility under the provisions of MD 12.3. Any questions regarding the individual's eligibility for IT Level I approval will be resolved in accordance with the due process procedures set forth in MD 12.3 Exhibit 1 and E. O. 12968.

In accordance with NRCAR 2052.204-70 "Security," IT Level I contractors shall be subject to the attached NRC Form 187 (See Section J for List of Attachments) which furnishes the basis for providing security requirements to prime contractors, subcontractors or others (e.g., bidders) who have or may have an NRC contractual relationship which requires access to or operation of agency sensitive information technology systems or remote development and/or analysis of sensitive information technology systems and data or other access to such systems and data; access on a continuing basis (in excess of 30 days) to NRC Headquarters controlled buildings; or otherwise requires NRC photo identification or card-key badges.

CONTRACTOR SECURITY REQUIREMENTS FOR LEVEL II

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

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

A contractor employee shall not have access to NRC facilities, sensitive information technology systems or data until he/she is approved by PERSEC/DFS first for temporary access (based on a favorable review of their security forms and checks) and final access (based on a favorably

adjudicated ANACI) in accordance with the procedures found in MD 12.3, Part I. The individual will be subject to a reinvestigation every 10 years. Timely receipt of properly completed security applications is a delivery order requirement. Failure of the contractor to comply with this condition within the ten work-day period may be a basis to void the notice of selection. In that event, the Government may select another firm for award.

The contractor shall submit a completed security forms packet (enclosed), including the SF-86, "Questionnaire for National Security Positions," and fingerprint charts, through the Project Officer to the NRC PERSEC/DFS for review and favorable adjudication, prior to the individual performing work under this contract. The contractor shall assure that all forms are accurate, complete, and legible (except for Part 2 of the questionnaire, which is required to be completed in private and submitted by the individual to the contractor in a sealed envelope), as set forth in MD 12.3. Based on PERSEC review of the applicant's security forms and/or the receipt of adverse information by NRC, the individual may be denied access to NRC facilities, sensitive information technology systems or data until a final determination is made of his/her eligibility under the provisions of MD 12.3. Any questions regarding the individual's eligibility for IT Level II approval will be resolved in accordance with the due process procedures set forth in MD 12.3 Exhibit 1 and E. O. 12968.

In accordance with NRCAR 2052.204-70 "Security," IT Level II contractors shall be subject to the attached NRC Form 187 (See Section J for List of Attachments) which furnishes the basis for providing security requirements to prime contractors, subcontractors or others (e.g. bidders) who have or may have an NRC contractual relationship which requires access to or operation of agency sensitive information technology systems or remote development and/or analysis of sensitive information technology systems and data or other access to such systems and data; access on a continuing basis (in excess of 30 days) to NRC Headquarters controlled buildings; or otherwise requires NRC photo identification or card-key badges.

CANCELLATION OR TERMINATION OF IT ACCESS/REQUEST

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

9.0 Project Officer Authority

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

Name: Louis Grosman

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

(1) Technical direction to the contractor which shifts work emphasis between areas of work or tasks, authorizes travel which was unanticipated in the Schedule (i.e., travel not contemplated in the Statement of Work or changes to specific travel identified in the Statement of Work), fills in details, or otherwise serves to accomplish the contractual statement of work.

(2) Provide advice and guidance to the contractor in the preparation of drawings, specifications, or technical portions of the work description.

(3) Review and, where required by the order, approval of technical reports, drawings, specifications, and technical information to be delivered by the contractor to the Government under the order.

(c) Technical direction must be within the general statement of work stated in the order. The project officer does not have the authority to and may not issue any technical direction which:

(1) Constitutes an assignment of work outside the general scope of the order.

(2) Constitutes a change as defined in the "Changes" clause of the blanket purchase agreement.

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

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

(5) Terminates the order, settles any claim or dispute arising under the order, or issues any unilateral directive whatever.

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

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

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

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

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

order action to be taken with respect thereto is subject to 52.233-1 - Disputes.

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

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

10. Place of Performance

The Contractor shall complete all of the work associated with this task either at the Contractor's own facilities and/or at the NRC Headquarters in Rockville, Md. Travel to other locations will not be required.