

ORDER FOR SUPPLIES OR SERVICES

PAGE OF PAGES

1

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

1. DATE OF ORDER 09-30-2002		2. CONTRACT NO. (If any) GS-35F-0079J		6 SHIP TO	
3. ORDER NO NRC-33-01-191-005		MODIFICATION NO		4. REQUISITION/REFERENCE NO. CIO01179 - 7/30/2002	
5. ISSUING OFFICE (Address correspondence to) U.S. Nuclear Regulatory Commission Division of Contracts Contract Management Center 1 Washington, DC 20555-0001				a. NAME OF CONSIGNEE U.S. Nuclear Regulatory Commission Office of the Chief Information Officer	
				b. STREET ADDRESS ATTN: Daniel Galik Mail Stop: T-6-F15	
				c. CITY Washington	
				d. STATE DC	
				e. ZIP CODE 20555-0001	
7. TO:				f. SHIP VIA	
a. NAME OF CONTRACTOR ALLIED TECHNOLOGY GROUP, INC.				8. TYPE OF ORDER	
b. COMPANY NAME ATTN: William P. Connor <i>William P. Connor</i>				<input type="checkbox"/> a. PURCHASE ORDER	
c. STREET ADDRESS 1803 Research Boulevard, 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 210-15-550-398 J1159 252A 31X0200.210 OBLIGATE: \$200,000				10. REQUISITIONING OFFICE Office of the Chief Information Officer	

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 Refer to the SOW.
		16. DISCOUNT TERMS N/A	
13. PLACE OF		FOR INFORMATION CALL: (No collect calls)	
a. INSPECTION Destination	b. ACCEPTANCE Destination	Donald A. King Office: (301) 415-6731	

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 the quotation of Allied Technology Group, Inc. (Allied), dated Sept. 12, 2002, with revision dated Sept. 24, 2002, which is hereby incorporated by reference and made a part hereof this delivery order, to provide the NRC with computer security services for its Security Technology Assessment, at the firm fixed unit price reflected in the Schedule of Prices/Costs for each task.</p> <p>TIN: 52-1603280 DUNS NO.: 62-122-5598</p> <p>NRC Project Officer - Daniel Galik - (301) 415-6595</p>					

SEE BILLING INSTRUCTIONS ON REVERSE	18. SHIPPING POINT		19. GROSS SHIPPING WEIGHT		20. INVOICE NO		\$519,788.00	SUBTOTAL	
	21. MAIL INVOICE TO								17(h) TOTAL (Cont. pages)
	a. NAME U.S. Nuclear Regulatory Commission Division of Contracts								17(i) GRAND TOTAL
	b. STREET ADDRESS (or P.O. Box) Attn: Donald A. King Mail Stop: T-7-12								
c. CITY Washington			d. STATE DC	e. ZIP CODE 20555-0001			\$519,788.00		

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

TEMPLATE - ADM001

OPTIONAL FORM NO. 347 (Rev. 6/01)
ADM002

CONTINUATION PAGE

B.1 SCHEDULE OF SUPPLIES OR SERVICES AND PRICE/COSTS

1 PROJECT TITLE

The title of this project is as follows:

“SECURITY TECHNOLOGY ASSESSMENT FOR NRC SENSITIVE INFORMATION PROCESSING REQUIREMENTS AND CLASSIFIED INFORMATION PROCESSING REQUIREMENTS”

2. BRIEF DESCRIPTION OF WORK

a) Brief description of work:

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

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

3. SCHEDULE

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

NRC-33-01-191-005 SECTION B

SCHEDULE OF SERVICES

CLIN 0001 -TASK 3.1 Project Management Plan

Labor Category	Rate	Hours	Dollars
Sr. Management Analyst(206C)	\$117.28	24	\$2,815
Sr. Systems Analyst (205C)	\$78.19	24	\$1,877
Sr. Consultant	\$117.28	8	\$938
Subtotal		56	\$5,630

CLIN 0002 - TASK 3.2 NRC Sensitive Information Processing Requirements Document

Labor Category	Rate	Hours	Dollars
Sr. Management Analyst(206C)	\$117.28	80	\$9,382
Sr. Systems Analyst (205C)	\$78.19	120	\$9,383
Sr. Consultant	\$117.28	80	\$9,382
Subtotal		280	\$28,148

CLIN 0003 - TASK 3.3 Market Survey Briefing

Labor Category	Rate	Hours	Dollars
Sr. Management Analyst(206C)	\$117.28	40	\$4,691
Sr. Systems Analyst (205C)	\$78.19	80	\$6,255
Sr. Consultant	\$117.28	408	\$4,691
Subtotal		160	\$15,638

NRC-33-01-191-005 SECTION B

CLIN 0004 - TASK 3.4 NRC Sensitive Information Processing Pilot Test

Labor Category	Rate	Hours	Dollars
Sr. Management Analyst(206C)	\$117.28	40	\$4,691
Sr. Systems Analyst (205C)	\$78.19	80	\$6,255
Sr. Consultant	\$117.28	80	\$9,382
Software (Ceiling)			\$10,000*
Hardware (Ceiling)			\$35,000*
Subtotal		200	\$65,329

*Software and Hardware Ceiling amounts shall not be exceeded with NRC PO recommendation Contracting Officer approval.

CLIN 0005 - TASK 3.5 Network Infrastructure Security Technical Reports

Labor Category	Rate	Hours	Dollars
Sr. Management Analyst(206C)	\$117.28	80	\$9,382
Sr. Systems Analyst (205C)	\$78.19	80	\$6,255
Sr. Consultant	\$117.28	40	\$4,691
Subtotal		200	\$20,329

NRC-33-01-191-005 SECTION B

CLIN-0006 - TASK 3.6 Sensitive Information Processing Solution Implementation

Labor Category	Rate	Hours	Dollars
Sr. Management Analyst(206C)	[REDACTED]	[REDACTED]	\$11,259
Sr. Systems Analyst (205C)	[REDACTED]	[REDACTED]	\$9,383
Sr. Consultant	[REDACTED]	[REDACTED]	\$14,074
Hardware Costs			\$100,000*
Software Costs			\$250,000*
Subtotal		[REDACTED]	\$384,715

*Software and Hardware Ceiling amounts shall not be exceeded with NRC PO recommendation Contracting Officer approval.

TOTAL ALL TASKS **\$519,788**

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

B.2 CONSIDERATION AND OBLIGATION

(a) The total estimated amount of this contract(ceiling) for the products/services ordered, delivered, and accepted under this contract is \$200,000. The Contracting Officer may unilaterally increase this amount as necessary for orders to be placed with the contractor during the contract period provided such orders are within any maximum ordering limitation prescribed under this contract.

(b) The amount presently obligated with respect to this contract is \$200,000. The Contracting Officer may issue orders for work up to the amount presently obligated. This obligated amount may be unilaterally increased from time to time by the Contracting Officer by written modification to this contract. The obligated amount shall, at no time, exceed the contract ceiling as specified in paragraph (a) above. When and if the amount(s) paid and payable to the Contractor hereunder shall equal the obligated amount, the Contractor shall not be obligated to continue performance of the work unless and until the Contracting Officer shall increase the amount obligated with respect to this contract. Any work undertaken by the Contractor in excess of the obligated amount specified above is done so at the Contractor's sole risk.

NRC-33-01-191-005 SECTION B

B.3 PERIOD OF PERFORMANCE

This order shall be effective from September 30, 2002, through June 30, 2003.

NRC-33-01-179-020 SECTION B

B.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.

Item No.	Deliverable Description	Deliverable Due Date Project Start (September 30, 2002)
1	Kick-Off Meeting	5 workdays after award (project start, PS) or earlier (OCT 7, 2002)
2	Monthly Progress Reports	Monthly; 10 th day of each month November 14, 2002 December 13, 2002 January 15, 2003 February 14, 2003 March 14, 2003 April 14, 2003 May 14, 2003 June 13, 2003
3	Deliver Project Management Plan	PS + 15 workdays (OCT 22, 2002)
4	Deliver Draft NRC Sensitive Information Processing Requirements Document	PS + 45 workdays (DECEMBER 5, 2002)
5	Deliver Final NRC Sensitive Information Processing Requirements Document	10 workdays after approval of Draft
6	Deliver Market Survey Briefing	PS + 75 Workdays (JANUARY 21, 2003)
7	Deliver NRC Sensitive Information Processing Test Report	PS + 135 Workdays (APRIL 16, 2003)
8		
9	Deliver Network Infrastructure Security Technical Reports	5 days after tasked by Government Project Officer
10	Implement Operational Sensitive Information Processing Solution	30 Workdays after tasked by Government Project Officer (TBD)

4.4 Instructions for Deliverables

Deliverables shall be delivered on the dates specified in the task order. If for any reason a deliverable cannot be delivered within the scheduled time frame, the Contractor shall notify the NRC Contracting Officer and NRC Project Officer in writing with cause of delay and the proposed revised schedule. This notice shall include the impact on the overall project. The NRC Project Officer shall make a business decision about the impact of the delay and forward the impact to the Contracting Officer.

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 Officer 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 Project Manager, unless otherwise indicated. All deliverables shall be formatted and prepared using Corel WordPerfect software for the documentation and reports, and Microsoft Powerpoint for the briefings. 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.

NRC-33-01-191-005

SECTION C -DESCRIPTION/SPECIFICATIONS/STATEMENT OF WORK

NUCLEAR REGULATORY COMMISSION (NRC)

OFFICE OF THE CHIEF INFORMATION OFFICER (OCIO)

For

FY 2002

Security Technology Assessment

For NRC Sensitive Information Processing Requirements

September 26, 2002

SECTION C -DESCRIPTION/SPECIFICATIONS/STATEMENT OF WORK

1.0 INTRODUCTION

Background

The NRC Automated Information Systems (AIS) Security Program Policy (Management Directive 12.5) specifies that sensitive information requires protection from disclosure, alteration, and loss. It also currently states that encryption technology should be utilized to protect sensitive information, including unclassified safeguards information. Since September 11th, the NRC has established closer working relationships with other Federal agencies involved with homeland security. NRC has a requirement to process increasing amounts of sensitive information internally among specific individuals across the NRC local area network, and also externally with our licensees and other external organizations. The sensitive information may include privacy act data, law enforcement sensitive data, homeland security sensitive data, company proprietary information, and several other categories. However, the current NRC automated information systems environment does not provide adequate capability for users to securely protect their sensitive information, as it does not make use of desktop encryption technology or other appropriate security technology solutions such as secure INTRANETS, secure email, and other similar security solutions.

Contract Objective

The primary objective of this contract is to identify the most cost-effective security solutions that can be incorporated within the existing NRC network infrastructure, in order to provide the capability for NRC users to securely process and exchange sensitive information, both internally and with external customers. A secondary objective of this contract is to provide expert level security engineering technical support to the NRC, to assist in the analysis and assessment of security issues and problems associated with the existing NRC local area network infrastructure. Optional efforts included within this contract will involve implementation of the selected security solution for sensitive information processing.

2.0 SCOPE OF WORK

Major tasks associated with this SOW include:

- Develop a Project Management Plan.
- Develop an NRC Sensitive Information Processing Requirements Document that collects and documents the detailed NRC requirements for the secure processing of sensitive information.
- Conduct a market survey of the most promising security technology solutions that best fit the NRC automated information systems environment and requirements, for the processing of sensitive unclassified information.
- Select a sampling of the most promising security solutions for the secure

SECTION C - DESCRIPTION/SPECIFICATIONS/STATEMENT OF WORK

processing of sensitive information, and conduct technical assessments to validate which products best fit NRC requirements.

- Recommend a security solution for a pilot test implementation on the operational NRC network to address NRC secure processing of sensitive information among internal NRC users, and also with external organizations.
- Prepare briefings that explain the results of the market survey and technology assessments, to support the processing of sensitive unclassified information.
- Obtain the technology required and implement a pilot test on the internal NRC network for a test community of up to 10 users processing sensitive information, (to include an option to expand the pilot test to 25 users, or 50 users).
- Assist the government staff in conducting the sensitive information processing pilot test, providing training to the users, and assisting in the collection of pilot test data and customer satisfaction feedback.
- Develop a Pilot Test Report that documents lessons learned and recommendations for improvements or enhancements in order to resolve any shortcomings in the selected security technology solution for securely processing sensitive information.
- Depending on the results of the sensitive information processing Pilot Test and availability of funding, the contractor shall procure, install, operate, and maintain the hardware and software required to implement the sensitive information processing security solution for up to 25 users located within NRC headquarters, (with an additional optional effort to implement the solution for 50 users, 100 users, 150 users, or 200 users). **(Optional task)**
- Provide Network Infrastructure Security Technical Reports utilizing expert level security engineering support, in order to conduct assessments and analyses of emergent technical issues and problems identified by NRC staff, associated with the design or operation of the existing NRC local area network infrastructure.

3.0 TASKS.

The following are specific requirements.

3.1 Project Management Plan

The contractor shall develop a detailed project plan specifying at a minimum, the approach to be utilized for each task, contractor staffing plan, the milestones, start/end dates for each activity and their dependencies, and the deliverables, to fulfill the NRC's

SECTION C -DESCRIPTION/SPECIFICATIONS/STATEMENT OF WORK

sensitive information processing requirements.

3.2 NRC Sensitive Information Processing Requirements Document

To complete this task, the Contractor shall interview personnel from up to five NRC offices in order to collect the requirements associated with the processing of sensitive information. Each interview session with each of the offices will be scheduled and coordinated by the Government Project Officer. The requirements identification will initially focus on internal NRC requirements, but will also expand to include requirements associated with the secure exchange of sensitive information with external organizations such as the licensees. The NRC offices may include program office officials and staff, project management staffs, and programming/development personnel familiar with the LAN and major applications. Telephone interviews will be acceptable for those individuals located at NRC Regional offices. The Government Project Officer may also schedule interview sessions with up to 3 NRC licensees, which may be conducted via telephone or email. The minimum standard for the NRC Sensitive Information Processing Requirements Document specifies that it will include a detailed description of each requirement, with an analysis or explanation of any technical issues, problems, or limitations that may be associated with each requirement.

3.3 Market Survey Briefing

The contractor shall conduct a market survey to identify the security technology solutions that best match the sensitive information processing requirements of NRC, and the existing NRC network infrastructure products and technology. As a minimum standard for acceptance, any encryption technology that may be considered for potential use in NRC networks must also be in compliance with NIST/FIPS standards and requirements. Products that have completed security assessments or reviews by the National Information Assurance Process (NIAP), the NIST cryptographic module validation program, the NSA SPOCK process, or by other Government organizations, are preferable to any products that have not been reviewed by the Government. Security technology solutions or products that are in use at other Government agencies may also be considered in this market survey. Integrated security technology solutions that provide the capability to digitally sign and encrypt email, and to perform content filtering, and virus screening should also be considered. The contractor shall conduct analyses and assessments of up to five of the most promising security products that best match NRC requirements. The purpose of the assessments will be to verify the vendors' claims about their products, assess the technical features, strengths, and weaknesses of the products, and to validate that the products will work within the existing NRC networking infrastructure. As a minimum standard, the Market Survey Briefing will present the results of the analyses and assessments of the security products, and will identify and recommend the one security solution that best matches NRC sensitive information processing requirements.

3.4 NRC Sensitive Information Processing Pilot Test

The contractor shall obtain the hardware and software to implement the identified sensitive information processing solution as a pilot test at NRC headquarters. The contractor is

SECTION C -DESCRIPTION/SPECIFICATIONS/STATEMENT OF WORK

encouraged to lease, borrow or pursue other options that may be available to obtain the needed hardware and software, in order to minimize the costs. This pilot test will be for a group of 10 NRC users that have urgent requirements to securely process sensitive information internally within NRC, and also externally with the licensees and other organizations. As a minimum standard, the initial focus of the pilot test will be on conducting a pilot to satisfy at least the internal NRC sensitive information processing requirements. Ideally, the security solution selected for this pilot test will also be capable of satisfying NRC requirements to securely exchange sensitive information externally also. The contractor shall work with the Government Project Officer who will assist the contractor by coordinating with NRC staff to integrate the solution into the NRC network infrastructure. The contractor shall provide documentation about the technical details of the product installation efforts, in order to allow NRC to understand how the installed solution impacts the security and accreditation status of the existing NRC network infrastructure. The contractor shall provide training to the users in the pilot test and assist with the resolution of any issues and problems that may be encountered as a result of the product being installed at NRC. All attempts will be made to minimize any disruptions to the existing NRC network infrastructure. The Government Project Officer will help to facilitate with the close coordination that will be required with the NRC OCIO LAN network infrastructure team. It is anticipated that the pilot test will last for a minimum of 30 days, during time which the contractor shall collect any user feedback. As a minimum standard, the NRC Sensitive Information Processing Pilot Test Report document will contain user feedback, the identification of technical issues that need to be resolved, lessons learned, and any recommended enhancements that could assist in improving the performance of the product in the pilot test. The Test Report will also identify the resources, recommend product lease/buy alternatives, or discuss any other issues that will need to be addressed in order to deploy the solution to a much larger community of users at NRC.

3.5 Network Infrastructure Security Technical Reports

The NRC has a requirement to quickly assess the security impact of any emergent problems or issues that may be identified with the design or operation of the NRC local area network infrastructure. The proposed addition of new technologies, or the introduction of new software applications, or the identification of a new security vulnerability, may all require the NRC Senior IT Security Officer to provide a technical recommendation that helps resolve any issue or problem identified. The contractor shall be tasked by Government Project Officer (via email, or via written memo), to deliver up to five Network Infrastructure Security Technical Reports. As a minimum standard, each Network Security Technical Report shall be no longer than five pages, and shall provide an expert level security engineering analysis or assessment of each issue or problem identified by the Government Project Officer, and shall recommend a solution or propose a strategy that will mitigate or help resolve the identified issue or problem.

3.6 Sensitive Information Processing Solution Implementation

Depending on the results of the sensitive information processing Pilot Test and availability of funding, the contractor shall procure, install, operate, and maintain the hardware and software required to implement the sensitive information processing security solution for up to 25 users

SECTION C -DESCRIPTION/SPECIFICATIONS/STATEMENT OF WORK

located within NRC headquarters, (with an additional optional effort to implement the solution for 50 users, 100 users, 150 users, or 200 users). The Government Project Officer will coordinate with the appropriate set of NRC users and the local area network infrastructure team to facilitate all actions required for the contractor to install the security solution. The contractor will provide support to the users, and assist the Government in the operation and maintenance of the solution. This effort will be for a period of up to 3 months, while the Government determines the best approach to continue support for the effort beyond 3 months.

4.0 Existing NRC Infrastructure Parameters

The contractor shall propose security solutions that are compatible with NRC's existing desktop infrastructure, and laptop environment. The current standard NRC desktop hardware configuration is an IBM compatible workstation with an Intel Pentium III processor or higher (500 MHz or greater). The standard workstations have 128mb RAM, 10G hard drives, and an Intel Pro 100B LAN card. The architecture supports PCI and AGP video. The agency workstation standard is NT 4.0, (expected to upgrade to Windows XP in FY 2004) and NRC currently supports two SQL databases as its standard, SQL 7.0 and Sybase™ 12. The agency standard O/S is currently Novell 4.6.1 (expected to upgrade to Novell 6 in FY 2004).

Current NRC software infrastructure:

- ▶ Microsoft Windows NT 4.00.1381, Service pack 6a;
 - ▶ NT Client Agent;
 - ▶ Microsoft SQL server 7.0 and SQL drivers for NT;
 - ▶ Novell NetWare Client for Windows NT/2000;
 - ▶ Diskkeeper;
 - ▶ Ensemble 1.22;
 - ▶ Informs 4.3;
 - ▶ Watermark 3.1.1.2;
 - ▶ Microshield v.5;
 - ▶ Network Access Suite 3.0;
 - ▶ Norton AntiVirus Corporate Edition;
 - ▶ PeopleSoft People Tools 7.57;
 - ▶ Corel WordPerfect 8.0.0;
 - ▶ Corel Presentations 8.0.0;
 - ▶ Corel QuattroPro 8.0.0;
 - ▶ GroupWise 5.5.3;
 - ▶ Netscape Communicator 4.7;
 - ▶ ADAMS 3.1.1 (custom); and
 - ▶ FTP Corp's Onnet 32 tools suite (includes FTP, 3270, Telnet, ping, etc.).

4.1 Kick-Off Meeting

SECTION C -DESCRIPTION/SPECIFICATIONS/STATEMENT OF WORK

Kick-Off meetings will be held to introduce the NRC Project Officer for each of the tasks and subtasks. The meetings will be held at NRC headquarters, Rockville Pike, Rockville, Maryland.

4.2 Monthly Progress Reports

The Contractor shall provide the NRC Project Officer and NRC Contracting Officer with a written monthly progress report. These are due to the NRC on the 10th day of each calendar month, throughout the project's duration. 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 Table of Deliverables and Schedule of Delivery

The Contractor shall submit deliverables by the due dates summarized in the table in subsection B. Deliverable due dates are based on workdays.

5.0 ORDER TERMS, CONDITIONS, AND REQUIREMENTS

5.1 PERFORMANCE REQUIREMENTS

The deliverables required under this order must conform to the standards contained, or referenced, in the statement of work. The Performance Requirements Summary outlines the performance requirements, deliverables, acceptable standards, surveillance method, and incentives and deductions applicable to this order (Attachment No. 2).

5.2 PLACE OF PERFORMANCE

Place of performance shall be at NRC headquarters, Rockville, Maryland.

5.3 TRAVEL

Travel outside of the Washington DC area shall be approved by the Government. No travel requirements are anticipated with this contract.

5.4 REPORTING REQUIREMENTS

(a) Project Management Plan

SECTION C -DESCRIPTION/SPECIFICATIONS/STATEMENT OF WORK

The contractor shall submit a detailed **Project Management Plan** to cover tasks under each of the above noted Tasks. The plan shall show tasking and subtasking, milestones, labor categories and/or staff assigned and the projected number of hours estimated to complete each task/subtask by staff member. This plan shall be progressed at the above level of detail on a monthly basis for the duration of the task. The **Project Management Plan** shall also include dollars by labor category/assigned personnel which will support the contractor's estimate for each task executed under this contract.

(b) Monthly Reports

The contractor shall provide a Monthly Status Report to the NRC Project Officer and the Contracting Officer by the 10th of each month. Each monthly report shall include updates to the **Project Management Plan** (Work Breakdown Schedule) listing the reasons for changes, proposed adjustments and justification, cost and schedule impacts. The **Project Management Plan** shall be progressed with the latest hours/costs and submitted as part of the monthly report. If at any time the project deviates from 5% in cost or schedule from the project management plan, the contractor shall schedule an update with the NRC Project Officer. The report shall also contain the BPA number, or order number, and task; the period covered by the report; a summary of work performed during the reporting period for each task, including appropriate statistics and plans for the next reporting period; a discussion of project plans, hardware problems, current operational problems, and the proposed corrective action, and analysis of the impact on other tasks within the scope of the SOW; and a status of expenditures under the order for the reporting period, cumulative expenditures to date, funds obligated to date, and balance of funds required to complete the order.

5.5 SECURITY

- a. Security/Classification Requirements Form. The NRC Form 187 (See Attachment) 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. In the performance of work under this contract, the contractor shall ensure all Sensitive Unclassified Information (i.e., Safeguards, Official Use Only, and Proprietary), to include documents, material, and equipment, originated or generated by the performing organization shall

SECTION C -DESCRIPTION/SPECIFICATIONS/STATEMENT OF WORK

be handled and marked in accordance with NRC Management Directive Volume 12, "Security," Handbook 12.6, "NRC Sensitive Unclassified Information Security Program." Each subcontract and purchase order issued hereunder involving the generation of Sensitive Unclassified Information, as described above, shall include a provision to the effect that in the performance of such subcontract or purchase order, all Sensitive Unclassified Information, as described above, shall be handled and marked in accordance with NRC Management Directive Volume 12, "Security," Handbook 12.6, "NRC Sensitive Unclassified Information Security Program." Handbook 12.6 is attached to this statement of work.

- 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

SECTION C -DESCRIPTION/SPECIFICATIONS/STATEMENT OF WORK

- 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

SECTION C -DESCRIPTION/SPECIFICATIONS/STATEMENT OF WORK

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.
- l. 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.
- m. 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

SECTION C -DESCRIPTION/SPECIFICATIONS/STATEMENT OF WORK

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

SECTION C - DESCRIPTION/SPECIFICATIONS/STATEMENT OF WORK

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 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.

SECTION C -DESCRIPTION/SPECIFICATIONS/STATEMENT OF WORK

The contractor shall submit a completed security forms packet, including the SF-86, "Questionnaire for National Security Positions," and fingerprint charts, through the Project Officer to the NRC 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 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.

- n. **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.

SECTION C -DESCRIPTION/SPECIFICATIONS/STATEMENT OF WORK

5.6 BILLING INSTRUCTIONS

General: The contractor shall prepare vouchers or invoices as prescribed herein. FAILURE TO SUBMIT VOUCHERS/INVOICES IN ACCORDANCE WITH THESE INSTRUCTIONS WILL RESULT IN REJECTION OF THE VOUCHER/INVOICES AS IMPROPER.

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

Number of Copies: An original and three copies shall be submitted. Failure to submit all the required copies will result in rejection of the voucher/invoice as improper.

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

U.S. Nuclear Regulatory Commission
Division of Contracts and Property Management - T-7-I-2
Washington, DC 20555-0001

A copy of any invoice which includes a purchase of property valued at the time of purchase at \$5,000 or more, shall additionally be sent to:

Chief, Property Management Branch
Division of Facilities and Property Management
Mail Stop - T-7-D-27
Washington, DC 20555-0001

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

SECTION C -DESCRIPTION/SPECIFICATIONS/STATEMENT OF WORK

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

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

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

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

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

Preparation and Itemization of the Voucher/Invoice: To be considered a proper voucher/invoice, all of the following elements must be included:

1. BPA/Contract number and delivery order number.
2. Sequential voucher/invoice number.
3. Date of voucher/invoice.
4. Payee's name and address. (Show the name of the contractor and its correct address. In addition, when an assignment of funds has been made by the contractor, or a different payee has been designated, include the name and address of the payee). Indicate the name and telephone number of the individual responsible for answering questions which the NRC may have regarding the voucher/invoice.
5. Description of articles or services, quantity, unit price, total amount, and cumulative amount.

For labor-hour delivery orders with a ceiling, provide a breakdown by task of labor hours by labor category, hours, fixed rate, current period dollars, and cumulative hours and dollars billed to date as authorized under the

SECTION C -DESCRIPTION/SPECIFICATIONS/STATEMENT OF WORK

delivery order. For example:

Category	Current Hours	Fixed Rate	Current Billed	Cumulative	
				Hours	Total Billed
Sr. Scientist	100	35.00	\$3,500.00	500	\$ 17,500.00
Engineer	100	25.00	\$2,500.00	100	\$ 2,500.00
Totals:			\$6,000.00		\$ 20,000.00

Invoices for the order shall be broken down by task. You must also provide a consolidated summary (cover sheet) of the total amount billed inclusive of all tasks. The summary must contain the cumulative amount invoiced to date.

6. For contractor acquired property list each item purchased costing \$50,000 or more and having a life expectancy of more than 1 year and provide: (1) an item description, (2) manufacturer, (3) model number, (4) serial number, (5) acquisition cost, (6) date of purchase, and (7) a copy of the purchasing document.

7. Weight and zone of shipment, if shipped by parcel post.

8. Charges for freight or express shipments. Attach prepaid bill if shipped by freight or express.

9. Instructions to consignee to notify the Contracting Officer of receipt of shipment.

10. Travel Reimbursement (if applicable)

The contractor shall submit claims for travel reimbursement as a separate item on its fixed-price invoice/voucher in accordance with the following:

Travel reimbursement. Total costs associated with each trip must be shown in the following format:

<u>Start Date</u>	<u>Destination</u>	<u>Costs</u>
From:	From:	\$
To: To:		\$

Provide supporting documentation (receipts) for travel expenditures in excess of \$75.00 in an attachment to the invoice/voucher.

SECTION C -DESCRIPTION/SPECIFICATIONS/STATEMENT OF WORK

Billing of Cost After Expiration of Order: If costs are incurred during the delivery order period and claimed after the order has expired, the period during which these costs were incurred must be cited. To be considered a proper expiration voucher/invoice, the contractor shall clearly mark it "EXPIRATION VOUCHER" or "EXPIRATION INVOICE."

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

Supersession: These instructions supersede any previous billing instructions.

5.7 PROJECT OFFICER

The Contracting Officer's authorized technical representative hereinafter referred to as the project officer for this order is:

Name: Daniel Galik

Address: U.S. Nuclear Regulatory Commission
Mailstop T6-F15
Washington, DC 20555

Telephone Number: (301) 415-6595, FAX: (301) 415-5368

a. 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.

SECTION C -DESCRIPTION/SPECIFICATIONS/STATEMENT OF WORK

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 or associated BPA.
2. Constitutes a change as defined in the "Changes" clause of the GSA contract.
3. In any way causes an increase or decrease in the total fixed price or the time required for performance of any orders.
4. Changes any of the expressed terms, conditions, or specifications of the order or associated BPA.
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 CO. 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 CO.

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 CO in writing within five (5) working days after the receipt of any instruction or direction and shall request the CO to modify the order or associated BPA accordingly. Upon receiving the notification from the contractor, the CO shall issue an appropriate modification or advise the contractor in writing that, in the CO'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 or associated BPA.

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

SECTION C -DESCRIPTION/SPECIFICATIONS/STATEMENT OF WORK

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 CO 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 CO recommendations for approval, disapproval, or suspension of payment for supplies and services required under orders.
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.

The Technical Monitor for this order is:

Name: Louis Grosman

Address: U.S. Nuclear Regulatory Commission
Mailstop T6-F15
Washington, DC 20555

Telephone Number: (301) 415-5826 FAX: (301) 415-5826

- a. The Technical Monitor may issue technical instructions from time to time during the duration of this task order. Technical instructions must be within the general statement of work stated in the task order and shall not constitute new assignments of work or changes of such nature as to justify and adjustment in cost or period of performance. The contractor shall refer to Section G.17 of the basic task order for further information and guidance on any technical directions issued under this task order.

Any modifications to the scope-of-work, cost or period of performance of this task order must be issued by the Contracting Officer and will be coordinated with the OCIO Project Officer.

SECTION C -DESCRIPTION/SPECIFICATIONS/STATEMENT OF WORK

5.8 FAR 52.232-7, "PAYMENTS UNDER TIME-AND-MATERIAL AND LABOR-HOUR CONTRACTS"

FAR 52.232-7 is applicable and hereby incorporated by reference into this order.

5.9 FAR 52.227-14, "Rights in Data-General (June 1987)"

FAR 52.227-14 is applicable and hereby incorporated by reference into this order.

5.10 FAR 52.227-19, "Commercial Computer Software-Restricted Rights (June 1987)"

FAR 52.227-19 is applicable and hereby incorporated by reference into this order.

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

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

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

SECTION C -DESCRIPTION/SPECIFICATIONS/STATEMENT OF WORK

5.12 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 3. 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."

(END-OF-CLAUSE)

5.13 Compliance with U.S. Immigration Laws and Regulations

NRC contractors are responsible to ensure that their alien personnel are not in violation of United States Immigration and Naturalization (INS) laws and regulations, including employment authorization documents and visa requirements. Each alien employee of the Contractor must be lawfully admitted for permanent residence as evidenced by Alien Registration Receipt Card Form 1-151 or must present other evidence from the Immigration and Naturalization Services that employment will not affect his/her immigration status. The INS Office of Business Liaison

SECTION C -DESCRIPTION/SPECIFICATIONS/STATEMENT OF WORK

(OBL) provides information to contractors to help them understand the employment eligibility verification process for non-US citizens. This information can be found on the INS website, <http://www.ins.usdoj.gov/graphics/services/employerinfo/index.htm#obl>.

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

(End of Clause)

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

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

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

NRC-33-01-191-005

SECTION D - CONTRACT DOCUMENTS, EXHIBITS, OR ATTACHMENTS

LIST OF ATTACHMENTS

ATTACHMENT NUMBER	TITLE
1	SF3881, Payment Information Form ACH Vendor Payment System
2	NRC Management Directive Volume 12, "Security," Handbook 12.6, "NRC Sensitive Unclassified Information Security Program
3	SECURITY TECHNOLOGY ASSESSMENT FOR NRC SENSITIVE INFORMATION PROCESSING REQUIREMENTS AND CLASSIFIED INFORMATION PROCESSING REQUIREMENTS PERFORMANCE REQUIREMENTS SUMMARY

ACH VENDOR MISCELLANEOUS PAYMENT ENROLLMENT FORM

OMB No 1510-0056
Expiration Date 06/30/93

This form is used for Automated Clearing House (ACH) payments with an addendum record that contains payment-related information processed through the Vendor Express Program. Recipients of these payments should bring this information to the attention of their financial institution when presenting this form for completion.

PRIVACY ACT STATEMENT

The following information is provided to comply with the Privacy Act of 1974 (P.L. 93-579). All information collected on this form is required under the provisions of 31 U.S.C. 3322 and 31 CFR 210. This information will be used by the Treasury Department to transmit payment data, by electronic means, to vendor's financial institution. Failure to provide the requested information may delay or prevent the receipt of payments through the Automated Clearing House Payment System.

AGENCY INFORMATION

FEDERAL PROGRAM AGENCY

U.S. NUCLEAR REGULATORY COMMISSION

AGENCY IDENTIFIER

NRC

AGENCY LOCATION CODE (ALC)

31000001

ACH FORMAT

CCD+

CTX

CTP

ADDRESS

DIVISION OF ACCOUNTING AND FINANCE, MAIL STOP T-9 H4

WASHINGTON, DC 20555-0001

CONTACT PERSON NAME

FINANCIAL OPERATIONS SECTION

TELEPHONE NUMBER

(301) 415 - 7520

PAYEE/COMPANY INFORMATION

NAME

SSN NO. OR TAXPAYER ID NO.

ADDRESS

CONTACT PERSON NAME

TELEPHONE NUMBER

()

FINANCIAL INSTITUTION INFORMATION

NAME

ADDRESS

ACH COORDINATOR NAME

TELEPHONE NUMBER

()

NINE-DIGIT ROUTING TRANSIT NUMBER

DEPOSITOR ACCOUNT TITLE

DEPOSITOR ACCOUNT NUMBER

LOCK BOX NUMBER

ACH FORMAT

CHECKING

SAVINGS

LOCK BOX

SIGNATURE AND TITLE OF AUTHORIZED OFFICIAL

TELEPHONE NUMBER

()

Instructions for Completing SF 3881 Form

1. **Agency Information Section** — Federal agency prints or types the name and address of the Federal program agency originating the vendor/miscellaneous payment, agency identifier, agency location code, contact person name and telephone number of the agency. Also, the appropriate box for ACH format is checked.
2. **Payee/Company Information Section** — Payee prints or types the name of the payee/company and address that will receive ACH vendor/miscellaneous payments, social security or taxpayer ID number, and contact person name and telephone number of the payee/company. Payee also verifies depositor account number, account title, and type of account entered by your financial institution in the Financial Institution Information Section.
3. **Financial Institution Information Section** — Financial institution prints or types the name and address of the payee/company's financial institution who will receive the ACH payment, ACH coordinator name and telephone number, nine-digit routing transit number, depositor (payee/company) account title and account number. Also, the box for type of account is checked, and the signature, title, and telephone number of the appropriate financial institution official are included.

Burden Estimate Statement

The estimated average burden associated with this collection of information is 15 minutes per respondent or recordkeeper, depending on individual circumstances. Comments concerning the accuracy of this burden estimate and suggestions for reducing this burden should be directed to the Financial Management Service, Facilities Management Division, Property and Supply Branch, Room B-101, 3700 East West Highway, Hyattsville, MD 20782 and the Office of Management and Budget, Paperwork Reduction Project (1510-0056), Washington, DC 20503.

U.S. NUCLEAR REGULATORY COMMISSION

DIRECTIVE TRANSMITTAL

TN: DT-99-33

To: NRC Management Directives Custodians

Subject: Transmittal of Directive 12.6, "NRC Sensitive Unclassified Information Security Program"

Purpose: Directive and Handbook 12.6 have been revised to cross-reference MD 3.4, "Release of Information to the Public," and to include the use of Official Use Only cover sheets to facilitate identification or protection of unclassified information within NRC.

Office and Division of Origin: Office of Administration

Contact: Rhonda C. Bethea, 301-415-2254

Date Approved: June 2, 1998 (Revised: December 20, 1999)

Volume: 12 Security

Directive: 12.6 "NRC Sensitive Unclassified Information Security Program"

Availability: Rules and Directives Branch
Office of Administration
David L. Meyer (301)415-7162 or
Jeannette P. Kiminas (301)415-7086

***NRC Sensitive Unclassified
Information Security
Program***

***Directive
12.6***

Contents

Policy	1
Objective	1
Organizational Responsibilities and Delegations of Authority	1
Executive Director for Operations (EDO)	1
Chief Information Officer (CIO)	2
Inspector General (IG)	2
Deputy Executive Director for Management Services (DEDM)	2
Director, Office of Administration (ADM)	2
Office Directors and Regional Administrators	2
Director, Division of Facilities and Security (DFS), ADM	3
Applicability	3
Handbook	3
Exceptions or Deviations	3
References	3



U. S. Nuclear Regulatory Commission

Volume: 12 Security

ADM

NRC Sensitive Unclassified Information Security Program Directive 12.6

Policy (12.6-01)

All U.S. Nuclear Regulatory Commission personnel responsible for the safeguarding of sensitive unclassified information (e.g., Official Use Only information and unclassified Safeguards Information), other sensitive information, and activities involving this information must adhere to the authorities, responsibilities, and procedures specified in this directive and handbook. This directive and handbook do not affect Commission rules and regulations contained in the *Code of Federal Regulations* that are applicable to NRC licensees and others.

Objective (12.6-02)

To ensure that sensitive unclassified information is handled appropriately and is protected from unauthorized disclosure under pertinent laws, management directives, and applicable directives of other Federal agencies and organizations.

Organizational Responsibilities and Delegations of Authority (12.6-03)

Executive Director for Operations (EDO) (031)

Acts on appeals for denial of information requested under the Freedom of Information Act (FOIA) when the request involves information generated by offices reporting to the EDO, and acts on all appeals for denial of information requested under the Privacy Act.

Volume 12, Security
NRC Sensitive Unclassified Information Security Program
Directive 12.6

Chief Information Officer (CIO)
(032)

Directs and oversees NRC's information resources and information management.

Inspector General (IG)
(033)

Investigates instances of improper disclosure of information in violation of statutes and regulations.

**Deputy Executive Director for
Management Services (DEDM)**
(034)

As designated Senior Agency Official for information security matters, directs and administers the agency's information security programs.

Director, Office of Administration (ADM)
(035)

Provides overall NRC security program guidance and direction and ensures that NRC's security program is effectively and efficiently carried out by the NRC Division of Facilities and Security (DFS).

**Office Directors and
Regional Administrators**
(036)

- Ensure that NRC employees and NRC contractor personnel under their jurisdiction are cognizant of and comply with the provisions of this directive and handbook. (a)
- Advise DFS of any existing or proposed sensitive unclassified activities in organizations under their jurisdiction. Report any significant change or termination of sensitive unclassified activities to DFS for review of associated contracts, subcontracts, or similar actions. (b)
- Advise DFS of any information that indicates noncompliance with this directive and handbook or is otherwise pertinent to the proper protection of sensitive unclassified information. (c)
- Request exceptions to or deviations from this directive and handbook, as required. (d)

**Director, Division of Facilities and
Security (DFS), ADM
(037)**

Plans, develops, establishes, and administers policies, standards, and procedures for the NRC Sensitive Unclassified Information Security Program. Monitors reports of non-compliance and recommends corrective actions, as appropriate, to DEDM and office directors.

**Applicability
(12.6-04)**

This directive and handbook apply to all NRC employees and consultants and to all NRC contractors to whom they apply as a condition of a contract or a purchase order.

**Handbook
(12.6-05)**

Handbook 12.6 provides guidelines for the preparation, distribution, accountability, and safeguarding of sensitive unclassified information.

**Exceptions or Deviations
(12.6-06)**

Exceptions to or deviations from this directive and handbook may be granted by DFS except in those areas in which the responsibility or authority is vested solely with the Commission, the EDO, or with ADM, and is nondelegable; or for matters specifically required by law, Executive order, or directive to be referred to other management officials.

**References
(12.6-07)**

Atomic Energy Act of 1954, as amended (42 U.S.C. 2011 et seq.).

Code of Federal Regulations—

10 CFR Part 2, "Rules of Practice for Domestic Licensing Proceedings and Issuance of Orders."

10 CFR Part 9, "Public Records."

10 CFR Part 50, "Domestic Licensing of Production and Utilization Facilities."

10 CFR Part 51, "Environmental Protection Regulations for Domestic Licensing and Related Regulatory Functions."

References

(12.6-07) (continued)

- 10 CFR Part 70, "Domestic Licensing of Special Nuclear Material."
- 10 CFR Part 71, "Packaging and Transportation of Radioactive Material."
- 10 CFR 73.21, "Requirements for the Protection of Safeguards Information."
- 10 CFR 73.57, "Requirements for Criminal History Checks of Individuals Granted Unescorted Access to a Nuclear Power Facility or Access to Safeguards Information by Power Reactor Licensees."
- 10 CFR 73.71, "Reporting of Safeguards Events."
- 10 CFR Part 1017, "Identification and Protection of Unclassified Controlled Nuclear Information" (Department of Energy, General Provisions).
- Energy Reorganization Act of 1974, as amended (42 U.S.C. 5801 et seq.).
- "Freedom of Information Act" (5 U.S.C. 552).
- Inspector General Act (5 U.S.C. App. 3).
- NRC Management Directive 3.1, "Freedom of Information Act."
 - 3.2, "Privacy Act."
 - 3.4, "Release of Information to the Public."
 - 3.5, "Public Attendance at Certain Meetings Involving the NRC Staff."
 - 5.5, "Public Affairs Program."
 - 12.1, "NRC Facility Security Program."
 - 12.2, "NRC Classified Information Security Program."
 - 12.3, "NRC Personnel Security Program."
 - 12.4, "NRC Telecommunications Systems Security Program."
 - 12.5, "NRC Automated Information Systems Security Program."
- NUREG-0910, Rev. 3, "NRC Comprehensive Records Disposition Schedule."
- NUREG-0794, "Protection of Unclassified Safeguards Information" (October 1981).

Approved: June 2, 1998
(Revised: December 20, 1999)

References

(12.6-07) (continued)

NUREG/BR-0069, Rev. 2, "NRC Classification Guide for National Security Information Concerning Nuclear Materials and Facilities" (CG-NMF-2) (December 1991).

"Privacy Act" (5 U.S.C. 552a).

***NRC Sensitive Unclassified
Information Security
Program***

***Handbook
12.6***

Contents

Part I

Introduction	1
Purpose and Scope (A)	1
Applicability (B)	1
Authority for Controls (C)	2
Authority To Designate Sensitive Unclassified Information (D)	2
Release of Information to the Public (E)	2
Sensitive Unclassified Records in ADAMS (F)	3

Part II

Protection and Control of Sensitive Unclassified Information	4
Information Originated by NRC, NRC Contractors, or NRC Licensees (A)	4
Access (1)	4
When Information Is Marked (2)	6
How Information Is Marked (3)	7
Cover Sheet (4)	10
Reproduction (5)	10
Transmission (6)	11
Telecommunications (7)	13
Automatic Data Processing (ADP) (8)	15
Word Processing (9)	15
Protection of Information During Use (10)	15
Storage (11)	15
Destruction (12)	17
Removal of Information From the Sensitive Unclassified Category (13)	17
Information Originated by Sources Other Than NRC, NRC Contractors, or NRC Licensees (B)	21
General Rule (1)	21
Access (2)	22
Hearings, Conferences, or Discussions (C)	22
Security Preparations Required for Hearings, Conferences, or Discussions (1)	22
Where Held (2)	22
Protective Orders (D)	23

Contents (continued)

Exhibits

1	Safeguards Information	24
2	Information Not Subject to Safeguards Information (SGI) Controls	26
3	Safeguards Information Document Marking	27
4	Safeguards Information Cover Sheet	28
5	Proprietary Information Cover Sheet	29
6	Official Use Only Information Cover Sheet	30

Part I

Introduction

Purpose and Scope (A)

Requirements and procedures are given to ensure that sensitive unclassified information is adequately protected from unauthorized disclosure. (1)

“Sensitive unclassified information” is unclassified Safeguards Information (SGI), Official Use Only information, and Proprietary information. It also includes unclassified information from other Government agencies and sources outside of NRC and its contractors and licensees that requires special protective measures. Markings used by these agencies and sources include, for example, *For Official Use Only*, *Company Confidential*, and *Private*. (See Management Directive (MD) 12.4, “NRC Telecommunications Systems Security Program,” and Volume 12, “Glossary,” for a complete definition of “Sensitive Unclassified Information.”) (2)

The provisions of this part apply to information determined or verified by NRC to be Proprietary and information said to be Proprietary. The use of the words “sensitive unclassified information” or “Proprietary” includes both information determined or verified by NRC to be Proprietary and information said to be Proprietary. (3)

The specific types of information and documents that constitute SGI are specified in Exhibit 1 to this handbook. This list is not intended to be all-inclusive. Exhibit 2 specifies types of information not subject to SGI controls. (4)

Applicability (B)

NRC employees, consultants, and contractors are responsible for ensuring that the procedures specified in this part are followed to protect sensitive unclassified information. The use of the word “contractor” in this part includes subcontractors.

Authority for Controls (C)

The primary authorities for the protection of sensitive unclassified information are the Freedom of Information Act (5 U.S.C. 552), the Privacy Act (5 U.S.C. 552a), and 10 CFR Parts 2 and 9. SGI is controlled in accordance with Section 147 of the Atomic Energy Act of 1954, as amended, and 10 CFR 73.21.

Authority To Designate Sensitive Unclassified Information (D)

To designate information as “sensitive unclassified,” a determination must be made that one or more of the statutes and/or regulations mentioned in Section (C) of this part apply. This designation signifies that the information must receive limited distribution and must be protected from unauthorized disclosure. For matters of the Office of the Inspector General, the Inspector General is the only official authorized to designate documents as sensitive unclassified information under applicable statutes. (1)

Within NRC, branch chiefs and above, or other level deemed appropriate by an office director and issued in writing, are authorized to designate information as SGI. Within contractor organizations, the NRC contracting office’s authorized representative or the NRC project officer, when necessary, authorizes employees to perform this function. (2)

NRC branch chiefs and above and personnel appointed by NRC contractors are authorized to designate information as “Official Use Only” or “Proprietary.” (3)

Release of Information to the Public (E)

The presence of markings such as “Safeguards Information,” “Official Use Only,” “Proprietary,” or other similar markings, or the lack of markings does not determine whether a document may be withheld from the public. A review must be made of each sensitive unclassified document requested to determine whether the document is releasable. (See MD 3.4, “Release of Information to the Public.”) (1)

Whenever an office has a question regarding releasability, it may be appropriate to consult with—(2)

Release of Information to the Public (E) (continued)

- The Division of Information Management, Office of the Chief Information Officer (OCIO), if the Freedom of Information Act (FOIA) or the Privacy Act is involved (see MDs 3.1, "Freedom of Information Act," and 3.2, "Privacy Act") or the release of information relates to the NRC's public health and safety mission (see MD 3.4, "Release of Information to the Public") (a)
- The Office of Nuclear Material Safety and Safeguards on whether a document contains SGI (b)
- The Office of Nuclear Reactor Regulation on safeguards technical and regulatory reviews or generic reactor safeguards issues (c)
- The Office of the General Counsel on legal questions (d)
- Other responsible offices within NRC (e)
- The originator (f)

Other Government agencies or other sources should be consulted before documents bearing restrictive markings or containing sensitive unclassified information of primary interest to them are released to the public. (3)

When sensitive unclassified documents are requested under FOIA or the Privacy Act, the Freedom of Information Act and Privacy Act Officer, OCIO, will assist offices in determining if the documents fall within the scope of the request and consult with other Federal agencies or other sources from which the information is derived regarding their documents or information in NRC files. (See MDs 3.2, "Privacy Act," and 3.1, "Freedom of Information Act.") (4)

Sensitive Unclassified Records in ADAMS (F)

Documents created in the Agencywide Documents Access and Management System (ADAMS) containing or said to contain Proprietary information must be generated using the Proprietary template. For Official Use Only information, use the Official Use Only template to facilitate identification or protection of the information. The template should be used to safeguard unclassified information that may be exempted from public disclosure under FOIA or the Privacy Act and may be used to protect other unclassified information subject to conditional release (e.g., predecisional information). SGI may not be placed in ADAMS.

Part II

Protection and Control of Sensitive Unclassified Information

Information Originated by NRC, NRC Contractors, or NRC Licensees (A)

The procedures set forth in this section apply to Safeguards Information (SGI), Official Use Only, and Proprietary information.

Access (1)

NRC personnel and NRC contractor employees shall furnish sensitive unclassified information to only those persons who need the information for the conduct of official business. (a)

If doubt exists as to whether it is proper to furnish information in any particular case, NRC personnel and NRC contractor employees shall consult the—(b)

- Originating office (If the information was originated by a contractor or a licensee, the originator or the NRC office administering the contract or license must be consulted.) (i)
- Office that has primary interest in the information (ii)
- Source from which the information was derived (iii)

If SGI is involved, NRC personnel or NRC contractor employees shall consult the Office of Nuclear Material Safety and Safeguards and the Office of Nuclear Reactor Regulation. (c)

If Proprietary or Official Use Only information is involved, NRC personnel or NRC contractor employees shall consult the—(d)

Approved: June 2, 1998
(Revised: December 20, 1999)

**Information Originated by NRC,
NRC Contractors, or NRC
Licensees (A) (continued)**

Access (1) (continued)

- NRC office originating the information (i)
- Office that has primary interest in the information (ii)
- Source from which the information was derived (iii)

An access authorization (security clearance) is not required for access to SGI or other sensitive unclassified information. However, the requirements of 10 CFR 73.57 mandate an FBI fingerprint check be conducted for access to SGI at a power reactor facility. (e)

No person may have access to SGI unless the person needs the information to conduct official business and the person is—(f)

- An employee, agent, or contractor of an applicant for a license, of an NRC licensee, of the NRC, or of the United States Government (i)
- A member of a duly authorized committee of the Congress (ii)
- The Governor of a State or his or her designated representative (iii)
- A representative of the International Atomic Energy Agency (IAEA) engaged in activities associated with the U.S./IAEA Safeguards Agreement who has been certified by the NRC (iv)
- A member of a State or local law enforcement authority that is responsible for responding to requests for assistance during safeguards emergencies (v)
- An individual to whom disclosure is ordered in accordance with 10 CFR 2.744(e) in connection with a domestic licensing proceeding (vi)

The office director or the regional administrator responsible for the document may authorize additional distribution of SGI related to activities conducted under the license. The individuals specified in the preceding list are normally considered to be trustworthy in view of their employment status. However, some discretion should be used in granting access if there is any indication that the proposed recipient would be unwilling or unable to provide the protection prescribed for SGI. (g)

Information Originated by NRC, NRC Contractors, or NRC Licensees (A) (continued)

When Information Is Marked (2)

Documents (including drafts and worksheets), other than for Official Use Only that contain sensitive unclassified information and require marking, must be marked upon origination.

SGI Documents (a)

Documents (including drafts and worksheets) known to contain SGI that are not so marked must be marked accordingly by persons authorized to designate information as "Safeguards Information."

- Documents dated before January 20, 1981, need not be marked until they are withdrawn from the files. (i)
- Documents dated before January 20, 1982, and clearly marked as 10 CFR 2.790(d) to indicate that they contain SGI must be secured as SGI without the alteration of their marking until they are withdrawn from the files for any reason. When withdrawn, these documents must be marked in accordance with this part. (ii)

Official Use Only Documents (b)

A document that contains information for Official Use Only must be marked when the originator believes that marking is essential to ensure proper handling and to ensure that all persons having access to the record will be aware that the—

- Document must not be publicly released. (i)
- Document must be distributed only to those who have a need-to-know to conduct official business. (ii)

Conditional Release Documents (c)

Some NRC documents may be released to the public when particular conditions have been met (e.g., a particular period of time has elapsed, a particular event has occurred, or an agency position has been officially approved). These documents are subject to conditional release and should be protected as Official Use Only until the specific condition has been met. While physical marking of conditional release documents may not be appropriate and is not required, the use of cover sheets marked "Official Use Only" is encouraged to facilitate their protection until they meet the condition for public release.

Information Originated by NRC, NRC Contractors, or NRC Licensees (A) (continued)

When Information Is Marked (2) (continued)

Proprietary Information Documents (d)

Documents received by NRC or NRC contractors that contain or are said to contain Proprietary information but that are not marked must be marked when marking is essential to ensure proper handling and to ensure that all persons having access to the information will be aware that the—

- Information must not be publicly released. (i)
- Information must be distributed only to those who have a need-to-know to conduct official business. (ii)

How Information Is Marked (3)

Safeguards Information (a)

At the time it is determined that a document contains SGI, originators must place the name, title, organization, signature, and date of the individual authorized to make an SGI determination and who has determined that the document contains SGI in the lower right corner of the face of the original document, as indicated in Exhibit 3 of this handbook. If the originator or approver of the document is the person authorized to make the determination and signs the document, that signature is sufficient. The signature in either case must appear on the face of the original copy of the document. Other copies may have a facsimile signature or a typed name. (i)

For a document containing SGI, originators must place the marking "SAFEGUARDS INFORMATION" conspicuously at the top and bottom of the page. Originators also must place the marking "Violation of protection requirements for SAFEGUARDS INFORMATION subject to CIVIL and CRIMINAL penalties" in the lower left corner of the face of the document. (ii)

Official Use Only (b)

Originators must place the marking "OFFICIAL USE ONLY" at the top and bottom of the page on the face of each document containing information for Official Use Only when that marking is required to

Information Originated by NRC, NRC Contractors, or NRC Licensees (A) (continued)

How Information Is Marked (3) (continued)

ensure proper handling. The marking "LIMITED INTERNAL DISTRIBUTION PERMITTED" must be placed in the lower left corner of the face of the document.

Proprietary Information (c)

Originators must place the words "PROPRIETARY INFORMATION" at the top and bottom of the page on the face of each document containing or said to contain Proprietary information.

Multiple Page Documents (d)

The "SAFEGUARDS INFORMATION, OFFICIAL USE ONLY," or "PROPRIETARY INFORMATION" markings must be placed at the top and bottom of—

- The outside of the front and back covers, if any (i)
- The title page, if any (ii)
- The first page of text, if there is no front cover or title page (iii)
- The outside of the back page, if there is no back cover (iv)
- Each page of a document containing sensitive unclassified information (v)

Portion-Marking (e)

Portion-marking is accomplished by clearly indicating the portions (e.g., titles, paragraphs, subjects, or pages) that contain sensitive unclassified information by placing the appropriate abbreviation (e.g., "SGI") in parentheses at the beginning or end of the portion.

Sensitive Unclassified Information (i)

Portion-marking is required for sensitive unclassified information when—

Information Originated by NRC, NRC Contractors, or NRC Licensees (A) (continued)

How Information Is Marked (3) (continued)

- A document contains several categories of sensitive unclassified information. Portion-marking indicates which portions (e.g., paragraphs, pages, and appendices) contain each category, that is, Safeguards Information, SGI; Official Use Only information, OOU; or Proprietary information, "PROPIN." The highest category of information contained in the document ("SGI" or in the absence of "SGI," "PROPIN") will be the overall marking used at the top and bottom of the portion. (a)
- A document contains both classified and sensitive unclassified information. Portion-marking indicates which portions contain each category. Portions (e.g., paragraphs) that contain both sensitive unclassified information and classified information must be marked with the applicable classification markings only (see Part I, Section (B)(3)(g) of Handbook 12.2, "NRC Classified Information Security Program"). If a document is declassified and sensitive unclassified information remains, the document must be marked in accordance with the requirements stated in this part. (b)

Safeguards Information (ii)

In addition to the overall marking, portion-marking is required for SGI contained in—

- Correspondence to and from the NRC, NRC contractors, and NRC licensees (a)
- Items listed in Exhibit 1 of this handbook (b)

Files or Folders (f)

Files and folders containing sensitive unclassified information must be marked front and back with the appropriate category marking (e.g., "SAFEGUARDS INFORMATION," "OFFICIAL USE ONLY INFORMATION," or "PROPRIETARY INFORMATION") upon creation or when extracted from an existing file system.

Transmittal Documents (g)

Documents (e.g., cover letters or memoranda) that do not in themselves contain sensitive unclassified information but are used to

Information Originated by NRC, NRC Contractors, or NRC Licensees (A) (continued)

How Information Is Marked (3) (continued)

transmit one or more documents containing this information must be marked to indicate the fact that sensitive unclassified information is contained in the documents transmitted. The marking (e.g., "SAFEGUARDS INFORMATION," "OFFICIAL USE ONLY," or "PROPRIETARY INFORMATION") indicating the category of information must be placed at the top and bottom of the first page of the transmittal document. Additionally, the following marking must be placed at the side or bottom of the transmittal document:

"Document transmitted herewith contains sensitive unclassified information. When separated from enclosures, this document is decontrolled."

Cover Sheet (4)

Each copy of a document containing SGI in the possession of NRC or NRC contractors must be covered by an SGI cover sheet (NRC Form 461, Exhibit 4). Documents containing or said to contain Proprietary information must be covered by a Proprietary information cover sheet (NRC Form 190, Exhibit 5), when necessary to prevent unauthorized access. (a)

Cover sheets should be used for Official Use Only information when their use facilitates identification or protection of the information. The Official Use Only cover sheet (NRC Form 190(x), Exhibit 6) should be used to safeguard unclassified information and may be used to identify and protect other information subject to conditional release. Cover sheets need not be used on documents that are in files. (b)

Reproduction (5)

A minimum number of copies of documents containing or said to contain sensitive unclassified information may be reproduced by holders to meet operational requirements without permission of the originator or the responsible office. Care must be taken to prevent unauthorized access during reproduction and in the disposition of matter containing sensitive unclassified information (e.g., unneeded copies or improperly prepared copies). (a)

**Information Originated by NRC,
NRC Contractors, or NRC
Licensees (A) (continued)**

Reproduction (5) (continued)

Whenever the originator wants to limit the further dissemination or reproduction of documents containing sensitive information, the following statement should be placed on the front of the document: "Reproduction or Further Dissemination Requires Approval of _____." (b)

If reproduction of sensitive unclassified information is requested, NRC Form 30, "Request for Administrative Services," or NRC Form 460, "Request for Graphics Services," should contain an explanation in the special instructions block that sensitive unclassified information is attached, and an asterisk should be placed in the "Unclassified" and "Other" blocks. This action must be taken to ensure proper handling of the document and proper disposal of any waste (see Section (A)(12) of this part). The requester shall ensure that the markings on documents submitted for reproduction are in black or red and dark enough to be reproduced. (c)

Transmission (6)

Methods Used (a)

Documents containing sensitive unclassified information must be transmitted by one of the following methods: (i)

- NRC messenger or NRC contractor authorized messenger or courier. NRC messengers and couriers shall be authorized to hand-carry sensitive unclassified information outside a facility by their division director or a higher level authority. NRC contractor personnel shall be authorized by the cognizant security office. (a)
- U.S. Postal Service First Class Mail, U.S. Postal Service Registered Mail, U.S. Postal Service Express Mail, or U.S. Postal Service Certified Mail (b)
- NRC headquarters interoffice mail or NRC pouch mail between NRC headquarters and regional offices (c)

Information Originated by NRC, NRC Contractors, or NRC Licensees (A) (continued)

Transmission (6) (continued)

- Any individual authorized access to the category of information involved (*d*)
- Other means approved by the Director, Division of Facilities and Security (DFS), Office of Administration (ADM) (*e*)

Individuals transporting documents containing SGI shall retain them in their possession at all times, unless they place the documents in the custody of another person authorized access to the information. (ii)

Individuals transporting documents containing other categories of sensitive unclassified information shall retain them in their possession to the maximum extent possible, unless they place the documents in the custody of another person authorized access to the information. Judgment must be used in handling these documents when retention is not feasible. (iii)

Preparation for Transmission (b)

General Rule (i)

- Documents containing sensitive unclassified information must be addressed to an individual authorized access to that information. (*a*)
- Material used for packaging must be opaque and of such strength and durability as to provide secure protection for the document in transit, prevent items from breaking out of the container, and facilitate the detection of any tampering with the container. (*b*)

Safeguards Information (ii)

- Documents containing SGI may be hand-carried or transmitted between NRC headquarters facilities by NRC interoffice mail, or between headquarters and regional offices by NRC pouch mail, in a single opaque envelope or wrapper. The envelope or wrapper must have the words "Safeguards Information" at the top and bottom on both sides and be addressed to the intended recipient, with a return address included. (*a*)

**Information Originated by NRC,
NRC Contractors, or NRC
Licensees (A) (continued)**

Transmission (6) (continued)

- Whenever documents containing SGI are transmitted outside an NRC facility or an NRC contractor facility by other means or to other destinations, they must be enclosed in two opaque sealed envelopes or similar wrappings. The inner envelope or wrapper must show the address of the intended recipient and the sender on the front and have the words "Safeguards Information" at the top and bottom on both sides. The outer envelope or wrapper must be addressed to the intended recipient, must contain the address of the sender, and must not bear any markings or indication that the document contains sensitive unclassified information. (b)

Proprietary Information or Official Use Only Information (iii)

Documents containing Proprietary or Official Use Only information must be transmitted between NRC facilities and outside NRC facilities or NRC contractor facilities in a single opaque envelope or wrapper. The single opaque envelope or wrapper must not bear any markings or indication that the document contains Proprietary or Official Use Only information. Two opaque envelopes or wrappers may be used as described in Section (A)(6)(b)(ii) of this part when the sender believes it necessary to ensure proper handling and protection.

Receipts (iv)

Receipts are not required for sensitive unclassified documents. However, NRC Form 253, "NRC Messenger/Courier Receipt," may be used if the sender wishes to ensure the delivery of the document.

Telecommunications (7)

General Rule (a)

- Utmost discretion must be used in the transmission of any sensitive unclassified information by electrical means. Mail channels are preferable. For further information, refer to Management Directive (MD) 12.4, "NRC Telecommunications Systems Security Program." (i)

Information Originated by NRC, NRC Contractors, or NRC Licensees (A) (continued)

Telecommunications (7) (continued)

- Proprietary and Official Use Only information must be encrypted if encryption is requested by the sender. **Note:** NRC telecommunications from the NRC Secure Communications Center are automatically encrypted and acceptable for transmission of sensitive unclassified information. (ii)
- To request encryption for messages sent through communication centers, the sender shall place the letters "EFTO" (Encrypt For Transmission Only) on the message form between the address and the text of the message. Messages containing SGI, Official Use Only, or Proprietary information must contain the words "SAFEGUARDS INFORMATION," "OFFICIAL USE ONLY," or "PROPRIETARY INFORMATION," as applicable, before the beginning of the text. (iii)

Safeguards Information (b)

SGI must be transmitted over protected telecommunications circuits approved by DFS. Unprotected circuits may be used only under emergency or extraordinary conditions. For the purpose of this requirement, emergency or extraordinary conditions are defined as any circumstances that require immediate communication in order to report, summon assistance for, or respond to a safeguards event or an event that has potential safeguards significance. Examples of these events include—(i)

- Safeguards events that must be reported as specified in 10 CFR 73.71 (i.e., unaccounted-for shipments, suspected thefts, unlawful diversion or radiological sabotage, or events that significantly threaten or lessen the effectiveness of safeguards) (a)
- Schedule changes, delays, or equipment breakdowns associated with the transport of spent fuel or Category I strategic special nuclear material (b)
- Failure or loss of safety-related equipment identified in the physical security plan as being vital (c)

The restriction on telecommunications applies to telephone, telegraph, teletype, communicating word processors, facsimile circuits, and radio (ii)

Information Originated by NRC, NRC Contractors, or NRC Licensees (A) (continued)

Automatic Data Processing (ADP) (8)

SGI and other sensitive data (e.g., personal data, proprietary data, or data that has a high potential for financial loss) may be processed or produced on Information Technology systems, provided that the systems meet the requirements of MD 12.5, "NRC Automated Information Systems Security Program."

Word Processing (9)

SGI and other sensitive data may be processed, stored, or produced on stand-alone personal computers or the NRC Local Area Network provided that the systems meet the criteria of MD 12.5.

Protection of Information During Use (10)

While in use, documents containing sensitive unclassified information must be under the control of an individual authorized access to such information by the individual's division or office director or regional administrator in order to limit access to persons who have a "need-to-know." This requirement is satisfied in the case of SGI if the immediate space in which the documents are held is attended by an authorized individual even though the information is not constantly being used. In the case of Proprietary and Official Use Only information, this requirement is satisfied when the information is not constantly being used by those means that the office or division has determined will prevent unauthorized access. DFS will aid in developing the most practical approach possible.

Storage (11)

Official Use Only and Proprietary Information (a)

Official Use Only and Proprietary information stored in NRC space (headquarters and regional offices) that has electronic access control approved by DFS or NRC contract guards on duty requires no additional physical security measures, unless—

- Specific storage requirements have been published under a Privacy Act system of records. (i)
- The holder deems additional protection (e.g., a locking cabinet) is necessary because of unusual circumstances or the sensitivity of the information (e.g., resident inspection sites). (ii)

Information Originated by NRC, NRC Contractors, or NRC Licensees (A) (continued)

Storage (11) (continued)

Safeguards Information (b)

SGI must be stored in a locked security storage container when unattended or not in actual use. (i)

As the term is used in this part, "security storage container" includes any of the following repositories: (ii)

- A steel filing cabinet equipped with a steel locking bar and a three-position changeable combination, GSA-approved padlock for storage in NRC headquarters and regional office buildings that have sufficient controls to prevent unrestricted access to the container. An NRC office that is occupied by employees during working hours and locked during nonworking hours (cleaning personnel may have keys, if necessary) would be considered to have sufficient access controls. This steel filing cabinet would not be considered adequate for a generally "public" area (e.g., a Public Document Room). (a)
- A security filing cabinet that bears a Test Certification Label on the side of the locking drawer, or on an interior plate, and that is marked as a "General Services Administration Approved Security Container." (b)
- A bank safe deposit box. (c)
- Other repositories that the Director, DFS, judges would provide adequate physical protection. (d)

Lock Combinations (c)

The lock combinations protecting any category of sensitive unclassified information must be limited to a minimum number of persons who have a "need-to-know" for operating purposes and are otherwise authorized access to the category of sensitive unclassified information in accordance with the provisions of this part. Combinations must be changed when placed in use, whenever a person having access no longer has an official "need-to-know," or at least once every year.

**Information Originated by NRC,
NRC Contractors, or NRC
Licensees (A) (continued)**

Storage (11) (continued)

Inspection of Out-of-Service Storage Repositories (d)

Security storage containers, desks, and other storage repositories to be removed for repair or maintenance, returned to the supplier, or otherwise taken out of service for any reason must be examined to ensure that no classified or sensitive unclassified documents remain therein.

Destruction (12)

Holders of sensitive unclassified information documents are responsible for destroying these documents when they are no longer required. Records of destruction are not required. Documents containing sensitive unclassified information must be destroyed by a method that will prevent reconstruction of the information in whole or in part (see NUREG-0910, "NRC Comprehensive Records Disposition Schedule"). (a)

Documents may be destroyed by tearing them into small pieces (i.e., several pages or documents torn into one-half inch pieces or smaller and thoroughly mixed), or by burning, pulping, pulverizing, shredding, or chemical decomposition. Within NRC headquarters, documents may be placed in receptacles designated for classified waste or receptacles approved by DFS for destruction of sensitive unclassified information. (b)

**Removal of Information From the Sensitive Unclassified
Category (13)**

Necessity for Review (a)

Periodic review of documents containing sensitive unclassified information to determine whether these documents should remain in this category is not required. This review is necessary only when specific circumstances require such action. Typically, a request for the information under the Freedom of Information Act or the Privacy Act would necessitate a review of this type.

Information Originated by NRC, NRC Contractors, or NRC Licensees (A) (continued)

Removal of Information From the Sensitive Unclassified Category (13) (continued)

Who May Remove Information From the Sensitive Unclassified Category (b)

Sensitive Unclassified Information Other Than SGI (i)

The following individuals may remove markings from documents containing sensitive unclassified information (other than SGI) when these individuals determine that the information is no longer in the sensitive unclassified category: (a)

- The originator, whose name appears on the document (1)
- His or her successor (2)
- A supervisor of either of the above (branch chief or above) (see Section (A)(13)(d) of this part) (3)

These individuals must be notified if any other persons remove this information from the sensitive unclassified category. (b)

SGI (ii)

Any individual authorized to determine that a document contains SGI may remove the marking or indicate that it may be removed whenever the information is no longer in this category, provided that the following individuals are informed: (a)

- The individual whose name appears on the document (1)
- His or her successor (2)
- A supervisor of either of the above (branch chief or above) or other level deemed appropriate by an office director and issued in writing (3)

The procedure set forth in Section (A)(13)(d) of this part must be followed. (b)

**Information Originated by NRC,
NRC Contractors, or NRC
Licensees (A) (continued)**

**Removal of Information From the Sensitive Unclassified
Category (13) (continued)**

Notification (c)

The person authorizing removal of a document from the sensitive unclassified information category or authorizing a change in the category shall so advise, to the extent feasible, the recipients of the document, who in turn shall so advise any subsequent recipient.

Marking (d)

When Information Is Marked (i)

The marking indicating a date or event for removal of the information from the sensitive unclassified category may be placed on documents upon origination or upon removal of the information from the sensitive unclassified category. The person taking the action shall place the following marking on the face of the document: (a)

Removed from sensitive unclassified information category
(on) or (after) _____

_____	_____	_____	_____
(Signature of person making determination)	(Title)	(Office)	(Date)

The date of cancellation of the marking or the event that will result in cancellation must be indicated. If a date or event is given, any possessor of the information may remove the sensitive unclassified information marking (e.g., "SAFEGUARDS INFORMATION," "OFFICIAL USE ONLY," or "PROPRIETARY INFORMATION") after the date or event has occurred. The last line must be completed with the signature, title, and office of the person authorizing the action and the date of authorization. (b)

**Information Originated by NRC,
NRC Contractors, or NRC
Licensees (A) (continued)**

**Removal of Information From the Sensitive Unclassified
Category (13) (continued)**

Change in Category (ii)

Documents must be marked to indicate a change of category, the person who is responsible for the change, and the date of the change. For example, if the document is removed from the SGI category but will still contain Official Use Only information, the SGI markings must be removed and the document marked "OFFICIAL USE ONLY" and "LIMITED INTERNAL DISTRIBUTION PERMITTED."

Removal of Markings (iii)

As a minimum, the sensitive unclassified information markings on the first page of text and on the outside of the front and back covers, if any, must be blacked out upon removal of a document from the sensitive unclassified information category or upon a change in the category. In the latter case, the new category must be inserted. If there are no covers, the marking must be blacked out or changed on the title page. If there is no title page, the marking must be blacked out or changed on the first page of text and on the outside of the back page. (a)

Persons possessing copies of the document, except as stated below, who are advised that the marking is no longer required or that the marking is changed, shall use a marker to blacken out or change the sensitive unclassified information markings, as appropriate, on the copies in their possession and indicate on each copy the authority for deleting or changing the markings. (b)

Large file rooms and copy distribution centers possessing multiple copies are not required to black out or change the markings but will maintain the notification of removal or change as a record of the action taken. Copies transmitted outside these rooms or centers must be marked to indicate their content. (c)

Information Originated by NRC, NRC Contractors, or NRC Licensees (A) (continued)

Removal of Information From the Sensitive Unclassified Category (13) (continued)

Disagreement on Changes of Category (e)

In any instance in which a disagreement exists as to whether a document should be removed from the SGI category, the matter must be referred for final determination to the Director, Division of Fuel Cycle Safety and Safeguards, Office of Nuclear Material Safety and Safeguards, as the contact for issues related to materials and transportation, and to the Director, Division of Inspection Program Management, Office of Nuclear Reactor Regulation, as the contact for issues related to reactors. In other instances of disagreement as to the removal of sensitive unclassified information from a category or a change in the category, the matter should be referred to one of the persons specified in Section (A)(13)(b)(i) of this part.

Information Originated by Sources Other Than NRC, NRC Contractors, or NRC Licensees (B)

General Rule (1)

Sensitive unclassified information, originated by sources other than NRC, NRC contractors, or NRC licensees, must be protected and disseminated under the same security measures set forth in Section (A) of this part for sensitive unclassified information originated by NRC, NRC contractors, or NRC licensees. (a)

Documents originated by sources other than NRC, NRC contractors, or NRC licensees that are marked so as to indicate that they contain sensitive unclassified information (e.g., Company Confidential) must be marked with NRC standard markings to indicate the category of information (e.g., Proprietary information) when the holder determines this marking is necessary for clarification. Holders shall contact the originators of documents in these cases to ensure documents are properly marked. (b)

Information Originated by Sources Other Than NRC, NRC Contractors, or NRC Licensees (B) (continued)

Access (2)

If any doubt exists as to whether it is proper in any particular case to grant access to sensitive unclassified information originating outside NRC, NRC contractors, or NRC licensees, the originating party, or other appropriate person in the agency responsible for the information, or other source from which the information is derived, must be consulted.

Hearings, Conferences, or Discussions (C)

Security Preparations Required for Hearings, Conferences, or Discussions (1)

NRC personnel, NRC consultants, NRC contractor personnel, and others (e.g., bidders) who arrange or participate in hearings, conferences, or discussions (see MD 3.5, "Public Attendance at Certain Meetings Involving the NRC Staff") involving sensitive unclassified information shall—

- Ensure before a hearing, conference, or discussion that participating personnel are identified and are authorized to have access to the information to be discussed (a)
- Indicate to participating personnel that the specific data they will furnish is sensitive unclassified information and advise them of the category of the information (e.g., SGI, Official Use Only, or Proprietary information), together with any protective measures required (b)
- Ensure that no discussion takes place that is audible to persons not authorized access to the information (c)

Where Held (2)

With the exception of inspection exit interviews held at locations owned and controlled by NRC licensees, conferences involving sensitive unclassified information must be held within NRC guarded or controlled areas, if practical. Conferences may be held outside guarded or controlled areas only when the director of a headquarters office or a regional administrator determines that adequate protection can be provided such information.

Protective Orders (D)

Regulations, 10 CFR 2.740(c), for domestic licensing proceedings, provide authority to presiding officers to determine, on motion, whether a trade secret or other confidential research, development, or commercial information will not be disclosed or only will be disclosed in a designated way. This determination is contained in a protective order issued by the presiding officer that sets forth procedures necessary to protect the information.

Exhibit 1

Safeguards Information

The following categories of information and specific items are subject to controls for Safeguards Information (SGI) specified in Part II of this handbook:

- **Physical Protection at Fixed Sites (A)**

Unclassified information relating to the protection of facilities that possess formula quantities of strategic special nuclear material and power reactors,* specifically—

- Composite physical security plan for the nuclear facility or site (1)
- Site-specific drawings, diagrams, sketches, or maps that substantially represent the final design features of the physical protection system (2)
- Details of alarm system layouts showing location of intrusion detection devices, alarm assessment equipment, alarm system wiring, emergency power sources, and duress alarms (3)
- Written physical security orders and procedures for members of the security organization, as well as duress codes and patrol schedules (4)
- Details of the onsite and offsite communications systems that are used for security purposes (5)
- Lock combinations and mechanical key design (6)
- Documents and other material that contain lists or locations of certain safety-related equipment explicitly identified in the documents as vital for purposes of physical protection, as contained in physical security plans, safeguards contingency plans, or plant-specific safeguards analyses for production or utilization facilities (7)
- Composite safeguards contingency plan for the facility or site (8)
- Those portions of the facility guard qualifications and training plan that disclose features of the physical security system or response procedures (9)
- Response plans to specific threats detailing size, disposition, response times, and armament of responding forces (10)

* Most of the physical protection information for activities involving a formula quantity of unirradiated strategic special nuclear material would be National Security Information and classified in accordance with the NRC Classification Guide for National Security Information concerning Nuclear Materials and Facilities (CG-NMF-2)

Exhibit 1 (continued)

- **Physical Protection at Fixed Sites (A) (continued)**
 - Size, armament, and disposition of onsite reserve forces (11)
 - Size, identity, armament, and arrival times of offsite forces committed to respond to safeguards emergencies (12)

- **Physical Protection in Transit (B)**

Unclassified information relating to the protection of shipments of formula quantities of strategic special nuclear material and spent fuel, specifically—

- Composite transportation physical security plan (1)
- Schedules and itineraries for specific shipments* (2)
- Details of vehicle immobilization features, intrusion alarm devices, and communications systems (3)
- Arrangements with and capabilities of local police response forces, and locations of safe havens (4)
- Details regarding limitations of radio-telephone communications (5)
- Procedures for response to safeguards emergencies (6)

- **Inspections, Audits, and Evaluations (C)**

Unclassified information relating to safeguards inspections and reports, specifically, portions of safeguards inspection reports, evaluations, audits, or investigations that contain details of a licensee's or an applicant's physical security system or that disclose uncorrected defects, weaknesses, or vulnerabilities in the system.**

* Routes and quantities for shipments of spent fuel are not withheld from public disclosure. Schedules for spent fuel shipments may be released 10 days after the last shipment of a current series.

** Information regarding defects, weaknesses, or vulnerabilities may be released after corrections have been made. Reports of investigations may be released after the investigation has been completed, unless withheld pursuant to other authorities, for example, the Freedom of Information Act (5 U.S.C. 552).

Exhibit 2

Information Not Subject to Safeguards Information (SGI) Controls

Certain types of information, even though possibly regarded as SGI, are not subject to the provisions of Part II of this handbook. However, these items may require controls set forth in Part II of this handbook for other categories of sensitive unclassified information.

Most notably, these items include studies, reports, and analyses conducted by or on behalf of the Commission, licensees, or applicants for licenses concerning the safeguarding of nuclear materials or facilities. Information specifically excluded from protection as SGI under Part II of this handbook includes—

- Documents, drawings, or reports submitted by applicants or licensees, or produced by the staff, in response to the environmental and safety requirements contained in 10 CFR Parts 50, 51, 70, and 71 (1)
- Routes and quantities of spent fuel shipments (2)
- Information concerning licensee control and accounting procedures, or inventory differences (not otherwise classified as National Security Information or Restricted Data) for special nuclear material, or source material and byproduct material (3)
- Any information already in the public domain, including commercial safeguards equipment specifications, catalogues, and equipment buying data (4)
- Portions of guard qualification and training plans that do not disclose facility safeguards features or response procedures (5)

Note: Reports to or from the NRC that contain information concerning a licensee's physical protection program for special nuclear material not otherwise designated as SGI or classified as National Security Information or Restricted Data, shall be handled and marked as "PROPRIETARY INFORMATION" as defined by 10 CFR 2.790(d).

Exhibit 3

Safeguards Information Document Marking

SAFEGUARDS INFORMATION

Analysis of
Physical Security Plan
for
Sunshine Nuclear
Power Plant

Violation of protection requirements for
SAFEGUARDS INFORMATION subject
to CIVIL and CRIMINAL penalties. The
determination that this document contains
Safeguards information was made by

Name, Title, Organization, Date

SAFEGUARDS INFORMATION

Exhibit 4

Safeguards Information Cover Sheet

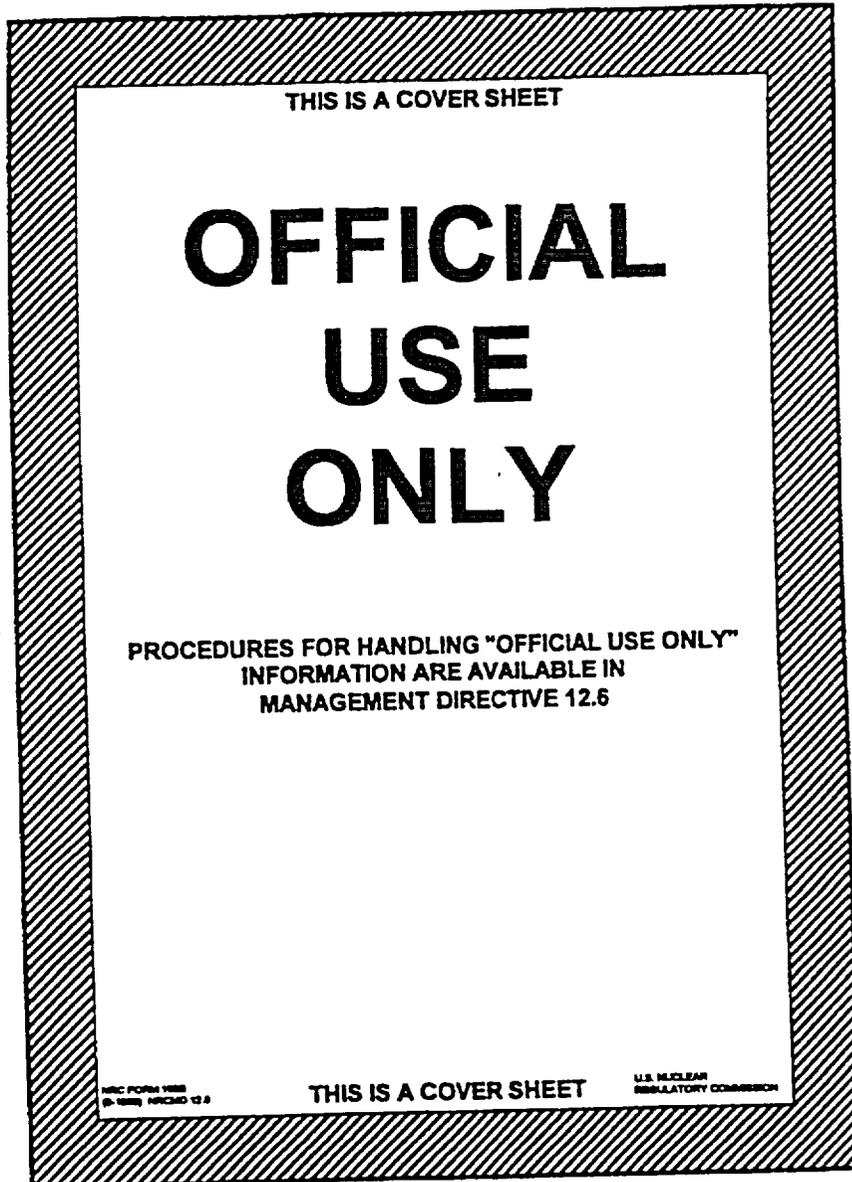
NRC FORM 463 (8-89)	U.S. NUCLEAR REGULATORY COMMISSION
SAFEGUARDS INFORMATION	
<p>THIS DOCUMENT CONTAINS INFORMATION WHICH MUST BE PROTECTED FROM UNAUTHORIZED DISCLOSURE IN ACCORDANCE WITH NRC REGULATIONS NRC MANUAL CHAPTER AND APPENDIX 2101 10 CFR 73.21 AND SECTION 147, ATOMIC ENERGY ACT OF 1954 AS AMENDED. APPLY VIOLATIONS ARE SUBJECT TO CIVIL OR CRIMINAL PENALTIES</p>	
<p>THIS DOCUMENT IS NOT TO BE LEFT UNATTENDED OR ACCESSIBLE TO UNAUTHORIZED PERSONS WHEN NOT IN USE IT MUST BE STORED IN A LOCKED SECURITY STORAGE CONTAINER</p>	
<p>IT IS YOUR RESPONSIBILITY TO PROTECT THE INFORMATION CONTAINED IN THIS DOCUMENT FROM COMPROMISE THEFT OR UNAUTHORIZED DISCLOSURE</p>	
SAFEGUARDS INFORMATION	

SECURITY TECHNOLOGY ASSESSMENT FOR NRC SENSITIVE INFORMATION PROCESSING REQUIREMENTS AND CLASSIFIED INFORMATION PROCESSING REQUIREMENTS PERFORMANCE REQUIREMENTS SUMMARY

Contract Requirement	Performance Standards	Method of Surveillance	Maximum Error Rate (MER) or Performance Requirement (PR)	Maximum Payment Percentage for Meeting or Exceeding the PR
<p>C.1 Project Management Plan</p> <p>The contractor shall develop a detailed Project Management Plan.</p>	<p>●Delivered by the due date. The plan shall specify at a minimum, the milestones, start/end dates for each activity and their dependencies, deliverables, to fulfill the NRC's sensitive information processing requirements.</p>	<p>●NRC PO Review</p>	<p>2%</p>	<p>1%</p>
<p>C.2 NRC Sensitive Information Requirements Document</p> <p>The Contractor shall interview NRC program office officials and staff, project management, security, and programming/development personnel familiar with the LAN and major applications.</p>	<p>●Delivered by the due date. Interview a representative set of NRC offices in order to collect the requirements associated with the processing of sensitive information.</p>	<p>●NRC PO Review</p>	<p>2%</p>	<p>5%</p>

Exhibit 6

Official Use Only Information Cover Sheet



Contract Requirement	Performance Standards	Method of Surveillance	Maximum Error Rate (MER) or Performance Requirement (PR)	Maximum Payment Percentage for Meeting or Exceeding the PR
<p>C.3 Market Survey Briefing</p> <p>The contractor shall conduct a market survey to identify the security technology solutions that best match the sensitive information processing requirements of NRC, and the existing NRC network infrastructure products and technology.</p>	<ul style="list-style-type: none"> ●Validate that the products will work within the existing NRC networking infrastructure. ●Deliver, by the due date. 	<ul style="list-style-type: none"> ●NRC PO Review 	2%	3%
<p>C.4 NRC Classified Information Processing Requirements Briefing</p> <p>The Contractor shall interview a representative set of NRC offices in order to collect the requirements associated with the processing of classified information.</p>	<ul style="list-style-type: none"> ●Deliver, by the due date, a draft and final versions of an NRC Classified Information Processing Requirements Briefing 	<ul style="list-style-type: none"> ●NRC PO Review 	2%	4%

Contract Requirement	Performance Standards	Method of Surveillance	Maximum Error Rate (MER) or Performance Requirement (PR)	Maximum Payment Percentage for Meeting or Exceeding the PR
<p>C.5 Network Infrastructure Security Technical Reports</p> <p>The contractor shall be tasked by Government Project Officer (via email, or via written memo), to deliver up to five Network Infrastructure Security Technical Reports</p>	<ul style="list-style-type: none"> ●As a minimum standard, each Network Security Technical Report shall be no longer than five pages, and shall provide an expert level security engineering analysis or assessment of each issue or problem identified by the Government Project Officer, . ●The Report shall recommend a solution or propose a strategy that will mitigate or help resolve the identified issue or problem. ●Deliver, by the due date. 	<ul style="list-style-type: none"> ●NRC PO Review 	<p>2%</p>	<p>5%</p>

Contract Requirement	Performance Standards	Method of Surveillance	Maximum Error Rate (MER) or Performance Requirement (PR)	Maximum Payment Percentage for Meeting or Exceeding the PR
<p>C.6 Sensitive Information Processing Solution Implementation (Optional task)</p> <p>Depending on the results of the sensitive information processing Pilot Test and availability of funding, the contractor shall procure, install, operate, and maintain the hardware and software required to implement the sensitive information processing security solution for up to 25 users located within NRC headquarters, (with additional optional effort to implement the solution for 50 users, 100 users, 150 users, or 200 users).</p>	<ul style="list-style-type: none"> ● Provide support for a period of up to 3 months ● Deliver, by the due date. 	<ul style="list-style-type: none"> ● NRC PO Review 	2%	74%

* Based on an MER of 12%

Exhibit 5
Proprietary Information Cover Sheet

NRC FORM 100 (9-1988) NRCMD 3.12	U.S. NUCLEAR REGULATORY COMMISSION
PROPRIETARY INFORMATION	
NOTICE	
THE ATTACHED DOCUMENT CONTAINS OR IS CLAIMED TO CONTAIN PROPRIETARY INFORMATION AND SHOULD BE HANDLED AS NRC SENSITIVE UNCLASSIFIED INFORMATION. IT SHOULD NOT BE DISCUSSED OR MADE AVAILABLE TO ANY PERSON NOT REQUIRING SUCH INFORMATION IN THE CONDUCT OF OFFICIAL BUSINESS AND SHOULD BE STORED, TRANSFERRED, AND DISPOSED OF BY EACH RECIPIENT IN A MANNER WHICH WILL ASSURE THAT ITS CONTENTS ARE NOT MADE AVAILABLE TO UNAUTHORIZED PERSONS	
COPY NO. _____	
DOCKET NO _____	
CONTROL NO _____	
REPORT NO. _____	
REC'D W/LTR DTD _____	
PROPRIETARY INFORMATION	