UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

OFFICE OF THE
GENERAL COUNSEL

October 24, 2003

Ann Marshall Young, Chair
Administrative Judge
Atomic Safety and Licensing Board
U.S. Nuclear Regulatory Commission
Mail Stop: T-F23
Washington, D.C. 20555

Thomas S. Elleman
Administrative Judge
Atomic Safety and Licensing Board
5207 Creedmoor Rd. #101
Raleigh, NC 27612

Anthony J. Baratta
Administrative Judge
Atomic Safety and Licensing Board
U.S. Nuclear Regulatory Commission
Mail Stop: T-3F23
Washington, D.C. 20555

In the Matter of
DUKE ENERGY CORPORATION
(Catawba Nuclear Station, Units 1 and 2)
Docket Nos. 50-413-OLA and 414-OLA

Dear Administrative Judges:

Pursuant to the Board's Order Confirming Matters Addressed at October 10, 2003, Telephone Conference (October 10, 2003), the NRC staff, by this letter, provides the Board the information it requested regarding handling of protected information. Enclosed are six documents that the Staff wishes to provide in response to the Board's request. The documents are: 1) the Requirements for the Protection of Safeguards Information (10 C.F.R. § 73.21); 2) *Standard Practice Procedures Plan Standard Format and Content for the Protection of Classified Matter for NRC Licensee, Certificate Holder, and Others Regulated by the Commission* (October 1999); 3) *NRC Regulatory Information Summary 2003-08 Protection of Safeguards Information from Unauthorized Disclosure* (April 2003); 4) *NRC Inspection Manual,Physical Protection Facility Approval and Safeguarding of National Security Information and Restricted Data;* 5) 10 C.F.R. Part 95; and, 6) *Minimum Requirements for Handling Classified and Sensitive Unclassified Information* (April 2003).

Sincerely,

Antonio Fernández
Counsel for NRC Staff

Enclosures: As stated

cc w/enclosures: A. Young, A. Baratta, T. Elleman, M. Olson
D. Repka, D. Curran, L. Vaughn

cc w/o encls: OCAA, SECY, ASLBP

Minimum Requirements for Handling Classified and Sensitive Unclassified Information

U.S. Nuclear Regulatory Commission

CLASSIFIED INFORMATION

CATEGORY OF INFORMATION	TRANSMISSION		CONTROL RECORDS	STORAGE	REPRODUCTION AUTHORITY	COVER SHEET	ACCESS AUTHORIZATION/ SECURITY CLEARANCE	CLASSIFICATION DESIGNATION AUTHORITIES
	INSIDE NRC HQ	OUTSIDE NRC and REGIONS						
TOP SECRET (RD & NSI)	Process through Top Secret Control Officer (415-2209)	Process through Top Secret Control Officer (415-2209)	Yes	Approval of Top Secret Control Officer	Approval of Top secret Control Officer	Yes SF 703 Orange	"Q" and Need-To-Know	Authorized Classifier
SECRET (RD & NSI)	Use NRC 188/A/B Use NRC 253, if Couriered	Use Two Opaque Envelopes-Registered Mail CMA Must be Used[1,3] (NRC 126)	Optional for Internal Use. Required for Transfer Outside the Agency (NRC 126)	Security Branch Approved Security Container	As Needed Unless Prohibited by Originator	Yes SF 704 Red	RD-"Q," NSI-"L" and Need-To-Know	Authorized Classifier
CONFIDENTIAL (RD & NSI)	Use NRC 188/A/B Use NRC 253, if Couriered	Use Two Opaque Envelopes-Certified Mail CMA Must be Used[1,3]	Optional	Security Branch Approved Security Container	As Needed Unless Prohibited by Originator	Yes SF 705 Blue	"L" and Need-To-Know	Authorized Classifier

Rev. 4/03

SENSITIVE UNCLASSIFIED INFORMATION

CATEGORY OF INFORMATION	TRANSMISSION		CONTROL RECORDS	STORAGE	REPRODUCTION AUTHORITY	COVER SHEET	ACCESS AUTHORIZATION/ SECURITY CLEARANCE	CLASSIFICATION DESIGNATION AUTHORITIES
	INSIDE NRC HQ	OUTSIDE NRC and REGIONS						
SAFEGUARDS INFORMATION	Use Single Opaque Envelope	Use Two Opaque Envelopes-First Class Mail[4]	No	File Cabinet with Locking Bar and Padlock	As Needed	Yes NRC 461	Need-To-Know	NRC Section Chiefs and Above Plus Designated Personnel
OFFICIAL USE ONLY (OUO)	Use Single Opaque Envelope	Use Single Opaque Envelope-First Class Mail	No	See Below[2]	As Needed	Yes NRC 190B	Need-To-Know	Originator
PROPRIETARY INFORMATION	Use Single Opaque Envelope	Use Single Opaque Envelope-First Class Mail	No	See Below[2]	As Needed	Yes NRC 190	Need-To-Know	Originator

Footnote: This chart contains minimum requirements. If conditions occur which do not meet one of these categories, consult NRC Management Directive 12.2, 12.6, or the Security Branch, Division of Facilities and Security.

1. When two opaque envelopes are required, the inner envelope must be addressed with an approved CMA and marked according to the highest category of classified or sensitive unclassified information it contains. Do not mark the outside envelope to indicate that the envelope contains classified or sensitive unclassified information.
2. Official Use Only and Proprietary Information stored in NRC space (headquarters and regional offices) with approved electronic access control or NRC contract guards requires no additional physical security measures unless—
   - Specific storage requirements have been published under a Privacy Act system of records, or
   - The employee possessing the information deems additional protection (e.g., a locking cabinet) necessary due to unusual circumstances or the sensitivity of the information (e.g., Resident Inspector sites.)
3. A commercial delivery company, approved by the CSA that provides nationwide, overnight service with computer tracking features.

   RD = Restricted Data
   NSI = National Security Information
   CMA = Classified Mailing Address
   CSA = Cognizant Security Authority
4. When two opaque envelopes are required, the inner envelope must be addressed with the name(s) of authorized individuals and marked according to the highest category of sensitive unclassified information it contains. Do not mark the outside envelope to indicate that the envelope contains sensitive unclassified information.

UNITED STATES
NUCLEAR REGULATORY COMMISSION
OFFICE OF NUCLEAR REACTOR REGULATION
OFFICE OF NUCLEAR MATERIAL SAFETY AND SAFEGUARDS
WASHINGTON, DC 20555-0001

April 30, 2003

NRC REGULATORY ISSUE SUMMARY 2003-08 PROTECTION OF SAFEGUARDS INFORMATION FROM UNAUTHORIZED DISCLOSURE

ADDRESSEES

All holders of operating licenses for nuclear power reactors, decommissioning reactor facilities, independent spent fuel storage installations, research and test reactors, large panoramic and underwater irradiators, and fuel cycle facilities.

INTENT

The U.S. Nuclear Regulatory Commission (NRC) is issuing this regulatory issue summary (RIS) and the attached Summary of Safeguards Information Requirements to inform addressees of the importance of protecting Safeguards Information from inadvertent release and unauthorized disclosure. The need to protect sensitive security information from inadvertent release and unauthorized disclosure which might compromise the security of nuclear facilities is heightened since the events of September 11, 2001. Addressees, including all cognizant personnel, have a continuing obligation to be mindful of their responsibilities in protecting such security information. Although many addressees have extensive experience in complying with applicable regulations related to handling and protection of Safeguards Information, additional licensees and individuals with limited or no experience in this area may now or soon will be covered by these requirements. This RIS is intended to serve as a consolidated source of information to reinforce the overall knowledge of Safeguards Information requirements as well as to highlight the serious consequences for failure to control and protect it.

Licensees are encouraged to broadly disseminate this information to affected employees and to post the attached Summary of Safeguards Information Requirements in areas where employees who handle Safeguards Information are located.

BACKGROUND

Several recent events involving published articles or comments to the media demonstrate the need for the NRC to reemphasize the importance of protecting Safeguards Information from inadvertent release and unauthorized disclosure. The release of this information, for example, could result in harm to the public health and safety and the Nation's common defense and security, as well as damage to the Nation's critical infrastructure, including nuclear power plants and other facilities licensed and regulated by the NRC.

ML031150743

SUMMARY OF ISSUE

Safeguards Information is a special category of sensitive unclassified information authorized by Section 147 of the Atomic Energy Act of 1954, as amended (the Act), to be protected. While Safeguards Information is considered sensitive unclassified information, it is handled and protected more like classified confidential information than like other sensitive unclassified information (e.g., privacy and proprietary information). Access to Safeguards Information is controlled by a valid need-to-know and an indication of trustworthiness normally obtained through a background check. The criteria for designating special nuclear material and power reactor information as Safeguards Information and associated restrictions on access to and protection of Safeguards Information are codified in Section 73.21 of Title 10 of the *Code of Federal Regulations* (10 CFR 73.21). Part 73 applies to licensees of operating power reactors, research and test reactors, decommissioning facilities, facilities transporting irradiated reactor fuel, fuel cycle facilities, and spent fuel storage installations. Examples of the types of information designated as Safeguards Information include the physical security plan for a nuclear facility or site possessing special nuclear material, the design features of the physical protection system, operational procedures for the security organization, improvements or upgrades to the security system, and vulnerabilities or weaknesses not yet corrected, and such other information as the Commission may designate by order. An example of additional information designated by order is the January 7, 2003 order to operating power reactor licensees concerning access authorization programs. That order made the details of NRC's enhanced access authorization requirements and licensee response to these requirements Safeguards Information. Another example is the April 29, 2003 order to operating power reactor licensees concerning security force training requirements.

In addition to the licensees subject to the Safeguards Information requirements of Part 73, and the types of information designated as Safeguards Information under those regulations, the Commission has authority under Section 147 to designate, by regulation or order, other types of information as Safeguards Information. For example, Section 147 allows the Commission to designate

> . . . a licensee's or applicant's detailed . . . security measures (including security plans, procedures and equipment) for the physical protection of source material or byproduct material, by whomever possessed, whether in transit or at fixed sites, in quantities determined by the Commission to be significant to the public health and safety or the common defense and security . . .

to be Safeguards Information. The Commission also may, by order, impose Safeguards Information handling requirements on these other licensees. An example of this type of order is the March 25, 2002 order to Honeywell International, a uranium conversion facility. Violations of Safeguards Information handling requirements, whether those of Part 73 or those imposed by order, are equally subject to the applicable civil and criminal sanctions, as discussed below and in the attached Summary of Safeguards Information Requirements.

Employees, past or present, and all persons who have had access to Safeguards Information have a continuing obligation to protect Safeguards Information against inadvertent release and unauthorized disclosure. The NRC staff and licensees have discovered several cases where Safeguards Information was inadvertently included in uncontrolled plant documents and documents intended for distribution to the public. Documents or other forms of communication

that include discussions about plant security should be reviewed carefully to ensure that Safeguards Information is not physically included or that plant security is not otherwise being compromised. Attachment 1 to this RIS further explains licensee and individual responsibilities under current regulations, issued Orders, and future Orders regarding the protection of Safeguards Information, and addresses penalties for inadequate protection and unauthorized disclosure.

Licensees are reminded that information designated as Safeguards Information must be withheld from public disclosure and must be physically controlled and protected. Physical protection requirements include (1) secure storage, (2) document marking, (3) access restricted to authorized individuals, (4) limited reproduction, (5) protected transmission, and (6) enhanced automatic data processing system controls. Changes are being proposed to NRC regulations applicable to Safeguards Information as a result of ongoing evaluations. Personnel security controls, including background checks and other means, are in effect for individuals authorized access to Safeguards Information, as is the strict adherence to the need-to-know principle.

Inadequate protection of Safeguards Information, including inadvertent release and unauthorized disclosure, may result in civil and/or criminal penalties. The Act explicitly provides in Section 147a that any person, whether or not a licensee of the Commission, who violates any regulations adopted under this section shall be subject to the civil monetary penalties of Section 234 of the Act. Furthermore, willful violation of any regulation or order governing Safeguards Information is a felony subject to criminal penalties in the form of fines or imprisonment, or both, as prescribed in Section 223 of the Act. The specific penalties associated with such violations will be determined by the staff in its implementation of the NRC Enforcement Policy, and the discretion of the Commission based on the details and significance of any violation. Statutory maximum penalties are addressed in Attachment 1.

The NRC will continue to evaluate its requirements, policies and guidance concerning the protection and unauthorized disclosure of Safeguards Information. Licensees and other stakeholders will be informed of proposed revisions or clarifications.

BACKFIT DISCUSSION

The RIS and the attachment do not request any action or written response; therefore, the staff did not perform a backfit analysis.

FEDERAL REGISTER NOTIFICATION

A notice of opportunity for public comment on this RIS was not published in the *Federal Register.*

PAPERWORK REDUCTION ACT STATEMENT

This RIS does not request any information collection and, therefore, is not subject to the Paperwork Reduction Act of 1995 (44 U.S.C. 3501 et seq.).

If you have any questions about this matter, please contact the person listed below.

/RA/
Charles L. Miller, Director
Division of Industrial and
Medical Nuclear Safety
Office of Nuclear Materials Safety
and Safeguards

/RA/
William D. Beckner, Program Director
Operating Reactor Improvements Program
Division of Regulatory Improvement Programs
Office of Nuclear Reactor Regulation

Contact: Bernard Stapleton, NSIR
(301) 415-2432
E-mail: bws2@nrc.gov

Attachments: 1. Summary of Safeguards Information Requirements
2. List of Recently Issued NRC Regulatory Issue Summaries

PAPERWORK REDUCTION ACT STATEMENT

This RIS does not request any information collection and, therefore, is not subject to the Paperwork Reduction Act of 1995 (44 U.S.C. 3501 et seq.).

If you have any questions about this matter, please contact the person listed below.

/RA/
Charles L. Miller, Director
Division of Industrial and
Medical Nuclear Safety
Office of Nuclear Materials Safety
and Safeguards

/RA/
William D. Beckner, Program Director
Operating Reactor Improvements Program
Division of Regulatory Improvement Programs
Office of Nuclear Reactor Regulation

Contact: Bernard Stapleton, NSIR
(301) 415-2432
E-mail: bws2@nrc.gov

Attachments: 1. Summary of Safeguards Information Requirements
2. List of Recently Issued NRC Regulatory Issue Summaries

ADAMS ACCESSION NUMBER: ML031150743 *See previous concurrence
DOCUMENT NAME: G:\RORP\OES\Staff Folders\Shapaker\0424JWS-0423-TReml-dRIS-NEW.wp

OFFICE	ISS:NSIR	ISS:NSIR	Tech Editor	D:DNS:NSIR	OGC
NAME	BWStapleton*	LASilvious*	PKleene*	GMTracy	JGoldberg
DATE	04/21/2003	04/22/2003	04/26/2003	04/30/2003	04/30/2003
OFFICE	MNS:NMSS	D:FCSS:FSPB:NMSSI	SC:OES:RORP:DRIP	PD:RORP:DRIP	OE
NAME	CLMiller	RCPierson	TReis	WDBeckner	JLuehman
DATE	04/30/2003	04/30/2003	04/30/2003	04/30/2003	04/30/2003

OFFICIAL RECORD COPY

SUMMARY OF SAFEGUARDS INFORMATION REQUIREMENTS

I. AUTHORITY

The Atomic Energy Act of 1954, as amended, 42 U.S.C. §§ 2011 *et seq.* (Act), grants the Nuclear Regulatory Commission broad and unique authority to prohibit the unauthorized disclosure of Safeguards Information upon a determination that the unauthorized disclosure of such information could reasonably be expected to have a significant adverse effect on the health and safety of the public or the common defense and security by significantly increasing the likelihood of theft, diversion, or sabotage of materials or facilities subject to NRC jurisdiction. Section 147 of the Act, 42 U.S.C. § 2167.

For licensees and any other person, whether or not a licensee (primarily 10 C.F.R. Part 50 reactor licensees, 10 C.F.R. Part 70 licensees for special nuclear material, and their employees and contractors) subject to the requirements in 10 C.F.R. Part 73, Safeguards Information is defined by NRC regulation as follows:

- *Safeguards Information* means information not otherwise classified as National Security Information or Restricted Data which specifically identifies a licensee's or applicant's detailed, (1) security measures for the physical protection of special nuclear material, or (2) security measures for the physical protection and location of certain plant equipment vital to the safety of production or utilization facilities.

10 C.F.R. § 73.2.

Specific requirements for the protection of Safeguards Information are contained in 10 C.F.R. § 73.21. Access to Safeguards Information is limited as follows:

> (c) *Access to Safeguards Information.* (1) Except as the Commission may otherwise authorize, no person may have access to Safeguards Information unless the person has an established "need to know" for the information and is:
>
> (i) An employee, agent, or contractor of an applicant, a licensee, the Commission, or the United States Government. However, an individual to be authorized access to Safeguards Information by a nuclear power reactor applicant or licensee must undergo a Federal Bureau of Investigation criminal history check to the extent required by 10 CFR 73.57;
>
> (ii) A member of a duly authorized committee of the Congress;
>
> (iii) The Governor of a State or designated representatives;
>
> (iv) 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;

> (v) A member of a state or local law enforcement authority that is responsible for responding to requests for assistance during safeguards emergencies; or
>
> (vi) An individual to whom disclosure is ordered pursuant to § 2.744(e) of this chapter [10 CFR 2.744(e)].
>
> (2) Except as the Commission may otherwise authorize, no person may disclose Safeguards Information to any other person except as set forth in paragraph (c)(1) of this section.

10 C.F.R. § 73.21(c).

The "need to know" requirement is specified by NRC regulation as follows:

> *Need to know* means a determination by a person having responsibility for protecting Safeguards Information that a proposed recipient's access to Safeguards Information is necessary in the performance of official, contractual, or licensee duties of employment.

10 C.F.R. § 73.2.

Thus, unless otherwise authorized by the Commission, NRC regulations limit access to Safeguards Information to certain specified individuals who have been determined to have a "need to know," i.e., specified individuals whose access has been determined to be necessary in the performance of official, contractual or licensee duties of employment.

Furthermore, except as otherwise authorized by the Commission, no person may disclose Safeguards Information to any other person unless that other person is one of the specified persons listed in 10 C.F.R. § 73.21(c)(1) and that person also has a "need to know." 10 C.F.R. § 73.21(c)(2). These regulations and prohibitions on unauthorized disclosure of Safeguards Information are applicable to all licensees and all individuals:

> This part [10 C.F.R. Part 73] prescribes requirements for the protection of Safeguards Information in the hands of any person, whether or not a licensee of the Commission, who produces, receives, or acquires Safeguards Information.

10 C.F.R. § 73.1(b)(7).

The Commission's statutory authority to protect and prohibit the unauthorized disclosure of Safeguards Information is even broader than is reflected in these regulations. Section 147 of the Act grants the Commission explicit authority to "issue such orders, as necessary to prohibit the unauthorized disclosure of safeguards information . . . ." This authority extends to information concerning special nuclear material, source material, and byproduct material, as well as production and utilization facilities.

The Act explicitly provides: "Any person, whether or not a licensee of the Commission, who violates any regulations adopted under this section shall be subject to the civil monetary penalties of Section 234 of this Act." Section 147a of the Act. Section 234a of the Act provides for a civil monetary penalty not to exceed $120,000 for each violation. *See* 10 C.F.R. § 2.205(j) (2003). Furthermore, a willful violation of any regulation or order governing Safeguards Information is a felony subject to criminal penalties in the form of fines or imprisonment, or both. *See* Sections 147b and 223a of the Act.

The NRC Enforcement Policy outlines potential NRC actions against both licensees and individuals for violations of the regulations and Orders using criteria that evaluate both the details and severity of the violation.

II. DISCUSSION

All licensees and all other persons who now have, or in the future may have, access to Safeguards Information must comply with all applicable requirements delineated in regulations and Orders governing the handling and unauthorized disclosure of Safeguards Information. As stipulated in 10 C.F.R. § 73.21(a), licensees and persons who produce, receive or acquire Safeguards Information are required to ensure that Safeguards Information is protected against unauthorized disclosure. To meet this requirement, licensees and persons subject to 10 C.F.R. § 73.21(a) shall establish and maintain an information protection system governing the proper handling and unauthorized disclosure of Safeguards Information. All licensees should be aware that since the requirements of 10 C.F.R. § 73.21(a) apply to all persons who receive Safeguards Information, they apply to all contractors whose employees may have access to Safeguards Information and they must either adhere to the licensee's policies and procedures on Safeguards Information or develop, maintain and implement their own information protection system, but the licensees remain responsible for the conduct of their contractors. The elements of the required information protection system are specified in 10 C.F.R. § 73.21(b) through (i). The information protection system must address, at a minimum, the following: the general performance requirement that each person who produces, receives, or acquires Safeguards Information shall ensure that Safeguards Information is protected against unauthorized disclosure; protection of Safeguards Information at fixed sites, in use and in storage, and while in transit; inspections, audits and evaluations; correspondence containing Safeguards Information; access to Safeguards Information; preparation, marking, reproduction and destruction of documents; external transmission of documents; use of automatic data processing systems; and removal of the Safeguards Information category.

As noted above, in addition to the responsibility of each licensee to ensure that all of its employees, contractors and subcontractors, and their employees comply with applicable requirements, all contractors, subcontractors, and individual employees also are individually responsible for complying with applicable requirements and all are subject to civil and criminal sanctions for failures to comply. The NRC considers that violations of the requirements applicable to the handling of Safeguards Information are a serious breach of adequate protection of the public health and safety and the common defense and security of the United States.

As a result, the staff intends to use the NRC Enforcement Policy, including the discretion to increase penalties for violations, to determine appropriate sanctions against licensees and individuals who violate these requirements. In addition, the Commission may use its discretion, based on the severity of the violation, to further increase the penalty for any violation up to the statutory maximum. Willful violations of these requirements will also be referred to the Department of Justice for a determination of whether criminal penalties will be pursued.

LIST OF RECENTLY ISSUED NRC REGULATORY ISSUE SUMMARIES

Regulatory Issue Summary No.	Subject	Date of Issuance	Issued to
2003-07	Issuance of Regulations Revising Filing Requirements for Advance Notification of the Shipment of Spent Nuclear Fuel and Special Nuclear Material	04/23/2003	All U.S. Nuclear Regulatory Commission (NRC) power reactor licensees, research and test reactor licensees, independent spent fuel storage installation licensees, and special nuclear material licensees who ship spent nuclear fuel and special nuclear material.
2003-06	High Security Protected and Vital Area Barrier/Equipment Penetration Manual	03/20/2003	All power reactor (including decommissioning reactor) licensees, independent spent fuel storage installation licensees, the conversion facility licensee, gaseous diffusion plant licensees, and Category I fuel cycle facility licensees.
2003-05	Issuance of Orders Imposing Additional Physical Protection Measures For Independent Spent Fuel Storage Installations Using Dry Storage	03/19/2003	All U.S. Nuclear Regulatory Commission (NRC) licensees who hold general licenses for independent spent fuel storage installations (ISFSIs) using dry storage pursuant to 10 CFR Part 72 and all applicants for site-specific licenses for ISFSIs pursuant to 10 CFR Part 72.
2003-04	Use of the Effective Dose Equivalent in Place of the Deep Dose Equivalent in Dose Assessments	02/13/2003	All U.S. Nuclear Regulatory Commission (NRC) licensees.

Note: NRC generic communications may be received in electronic format shortly after they are issued by subscribing to the NRC listserver as follows:

To subscribe send an e-mail to <listproc@nrc.gov >, no subject, and the following command in the message portion:

subscribe gc-nrr firstname lastname

OL = Operating License
CP = Construction Permit

NRC INSPECTION MANUAL NMSS

INSPECTION PROCEDURE 81820

PHYSICAL PROTECTION FACILITY APPROVAL AND SAFEGUARDING OF

NATIONAL SECURITY INFORMATION (NSI) AND RESTRICTED DATA (RD)

PROGRAM APPLICABILITY: 2681

81820-01 INSPECTION OBJECTIVE

To determine whether facilities approved for use and/or storage of NSI and RD are properly designed and managed to ensure that this material has the level of protection necessary for its sensitivity.

81820-02 INSPECTION REQUIREMENTS

02.01 Security Plan

a. Verify that the licensee/certificate holder follows the security plan submitted as part of the request for security facility approval. (10 CFR 95.15(b))

b. Verify that the licensee/certificate holder obtains prior NRC approval for any proposed change to the name, location, security procedures and controls, or floor plan of the approved facility (except as noted in 10 CFR 95.18(a)). (10 CFR 95.18(b))

02.02 Protection of NSI and RD

a. Protection while in use. Verify that, while in use, NSI and RD are kept under the direct control of an authorized individual. (10 CFR 95.27)

b. Verify that the licensee/certificate holder has established an accountability procedure for Secret matter. (10 CFR 95.41)

c. Storage of Secret matter. Verify that Secret matter that is unattended or not in actual use is:

1. Stored in a locked security container, and protected by an NRC-approved intrusion alarm.

2. Under the control of protective personnel.

The protective personnel must physically check security containers after the close of normal business and at least once every 8 hours thereafter, and protective personnel must be able to respond to an emergency situation within 15 minutes. (10 CFR 95.25)

d. Storage of Confidential matter. Verify that while unattended or not in actual use, Confidential matter is:

1. Stored in a locked security container within a locked room or building.

2. Protected by the same methods used for Secret matter (see Section 02.02c, above). (10 CFR 95.25(b))

e. Keys. Verify that the keys used to secure gates or doors in the perimeter of security areas are issued only to authorized persons. (10 CFR 95.25(i))

f. Protective Personnel. Verify that persons used to protect NSI or RD have the appropriate level of clearance. (10 CFR 95.31)

g. Lock Combinations. Verify that the following criteria are met:

1. Lock combinations are known only to the minimum number of people necessary for operating purposes, these people have a need-to-know, and they have the requisite clearance. (10 CFR 95.25(c)(1))

2. Lock combinations are changed when the container is put into use or taken out of use, when a person with knowledge of the combination no longer requires access, or when a combination may have been compromised; and if none of these conditions apply, the combinations are changed at least once a year. (CFR 95.25(c)(2))

3. Combinations are randomly selected using at least three numbers. (10 CFR 95.25(e))

4. When combination locks are closed, the dial is spun at least four times in the same direction. (10 CFR 95.25(f)(1))

5. Combinations are changed only by people cleared for access to the level of material in the container. (10 CFR 95.25(f)(2))

6. Names, addresses, and phone numbers of custodians and alternates are posted on the inside or outside of the container. (10 CFR 95.25(g)(1))

h. Unlocked Security Container. Verify, through a records check, that, when an unlocked security container is found unattended, the custodian or alternate is immediately notified, and the container is secured and inventoried by the next business day. (10 CFR 95.25(h))

i. Reproduction. Verify that Secret matter is not reproduced without the written permission of the originator, the originator's successor, or higher authority. (Confidential matter may be reproduced to the extent required by operational needs, unless such reproduction is otherwise restricted). (10 CFR 95.43)

j. Marking of Documents. Verify that the following criteria are met:

1. NSI and RD generated or possessed by the licensee/certificate holder are marked in accordance with classification guidance provided by the NRC. (If information is believed to be NSI or RD but has not yet been marked, it must be protected and marked pending review. A final determination of classification must be made within 30 days).

(10 CFR 95.37(a))

2. Document markings are consistent with their contents (10 CFR 95.37(b)), and the markings conform to 10 CFR 95.37 (c)-(e).

3. Each document contains portion marking. (10 CFR 95.37(f))

4. All Secret documents shall bear on the first page a properly completed documentation stamp. (10 CFR 95.37(g))

5. Transmittal letter markings are commensurate with the highest classified enclosure (sometimes the combination of enclosures may warrant a higher classification than either the enclosures or the transmittal letter). (10 CFR 95.37(h))

6. When material is discovered that is believed to be improperly classified or marked, the originator is notified and the material is protected at the highest level in question. (10 CFR 95.37(i))

7. Files, folders, binders, or groups of physically connected documents are marked with a classification at least as high as the highest classified document they contain. (10 CFR 95.37(j))

8. Drafts and working papers are marked on the top and bottom of each page with the highest classification contained in the document. (10 CFR 95.37(k))

9. Classified documents are downgraded according to NRC classification guides and appropriately marked. (10 CFR 95.45)

k. External Transmission. Verify that the following criteria are met:

1. Documents containing NSI and/or RD are transmitted only to Commission-approved security facilities. (10 CFR 95.39(a))

2. Documents containing NSI and/or RD transmitted outside the facility are appropriately marked and double-wrapped. (10 CFR 95.39(b))

3. Secret matter is transported by messenger-courier, registered mail, protective services approved by the Commission, or, under emergency conditions, by individuals possessing appropriate NRC or other Federal access authorization and written authority. (Confidential matter can be transported by these means or by first class, express, or certified mail). (10 CFR 95.39(c))

4. A telecommunication plan for a secure telecommunication system has been completed, submitted to, and approved by the NRC Division of Security prior to the transmission of any classified information. (10 CFR 95.39 (d))

l. Destruction. Verify that destruction of documents containing NSI or RD -- whether by burning, pulping, or another method -- ensures complete destruction of the material and precludes its recognition or reconstruction. (10 CFR 95.47)

m. Verify that when an employee's access authorization has been revoked in accordance with 10 CFR 25, the licensee/certificate holder has retrieved all materials containing NSI or RD from the individual and has taken steps to preclude the individual having future access. (10 CFR 95.51)

n. ADP. Has an ADP System Security Proposal been submitted to and approved by the NRC Division of Security prior to the processing of any classified data? (10 CFR 95.49)

02.03 Education

a. Verify that the licensee/certificate holder has established and maintains an effective security education program for those individuals possessing a U. S. Government personnel security access authorization. (10 CFR 95.33)

b. Verify that the security education program includes procedures to verify an individual's access authorization before NSI or RD is communicated to him/her. (10 CFR 95.33)

c. Verify that the security education program provides for continuing instruction as well as appropriate instruction for terminating employees. (10 CFR 95.33)

d. Verify that the security education program includes consideration and coverage of physical security features of the facility, the classified nature of the work, the classification and sensitivity of information, and an explanation of the "Classified Information Nondisclosure Agreement" (SF-312). (10 CFR 95.33)

02.04 Establishment of Security Areas. Verify that when a security area is established to protect NSI or RD, the following criteria are met:

a. It is separated from adjacent areas by a physical barrier to prevent unauthorized access (physical, audio, and visual).

b. Controls are established to prevent unauthorized access to and removal of classified matter.

c. Access is limited to authorized persons with a need for access.

d. Visitors without the appropriate access authorization are escorted at all times.

e. Badges or other means of identification are issued to each person when the number assigned to the area exceeds 30 persons.

f. Admittance is controlled by protective personnel during nonworking hours.

g. The protective personnel conduct tours of the area every 8 hours and continuously monitor points of access.

h. Entrances are continuously monitored by protective personnel or an approved alarm system. (10 CFR 95.29)

02.05 Access to NSI and/or RD

a. Verify that NSI and RD are released only to those persons who are properly authorized by the Commission to have access to it. (10 CFR 95.35(a))

b. Verify that access to NSI and RD is limited to those individuals who:

1. Have an established "need-to-know" the information. (10 CFR 95.35(a) (2))

2. Have a "Q" clearance for Secret RD or information containing intelligence information, CRYPTO, or other COMSEC(1) information, or have an "L" clearance for any other Secret or Confidential NSI or Confidential RD. (10 CFR 95 .35(a)(1)(I & ii))

3. Have NRC-approved storage facilities if these materials are to be transmitted to the individual. (10 CFR 95.35(a)(3))

c. Verify that the licensee/certificate holder denies access to or release of NSI to IAEA representatives except under the following conditions:

1. There is a written disclosure authorization from the NRC Division of Security. (10 CFR 95.36(a) and (c))

2. The IAEA representative has IAEA credentials and (a) is accompanied by a Commission employee, (b) has written confirmation of credentials for the specific visit, or (c) has credentials that can be verified by telephone communication with the Commission, (10 CFR 75.7).

3. The information is considered relevant to the conduct or the visit or inspection (10 CFR 95.36(a)). (Information containing RD should not be released to IAEA representatives). (10 CFR 95.36(a))

02.06 Termination of Facility Approval. The suspension, revocation, or termination of access authorization or security facility approval does not relieve any person from compliance with 10 CFR Part 95, if the security facility approval has been terminated by the Commission. (10 CFR 95.55)

a. Verify that the licensee/certificate holder immediately delivered all classified materials to the Commission, if the termination was in the interest of national security. (10 CFR 95.53(b))

b. Verify that the licensee/certificate holder delivered these materials to the Commission or to a person authorized to receive them, or destroyed the materials, if the termination of facility approval was for reasons other than national security. (10 CFR 95.53(a))

c. Verify that the licensee/certificate holder submitted a certificate of nonpossession of NSI and RD to the NRC Division of Security. (10 CFR 95.53(a) and

(b))

02.07 Notifications and Reports

a. Verify that the licensee/certificate holder promptly notifies the NRC Division of Security of any minor changes to the NRC-approved security facility plan. (10 CFR 95.18 (b))

b. Verify that the licensee/certificate holder immediately notifies the NRC Division of Security by telephone, followed up promptly in writing, when a request for security facility approval is withdrawn or cancelled. (10 CFR 95.21)

c. Verify that the licensee/certificate holder forwards a report to the appropriate NRC Regional Office (with a copy to NRC's Division of Security) of any instance of an unattended security container found open. (The report should describe actions taken to remedy the situation and prevent a recurrence). (10 CFR 95.25(h))

d. In instances where the licensee/certificate holder has changed a classification or declassified a document, or received notice of such change or declassification from the originator, verify that the licensee/certificate holder notifies other custodians who have received copies of the document from the licensee/certificate holder. (10 CFR 95.45(b))

e. Verify that the licensee/certificate holder immediately notifies the appropriate Regional Office of any of the following events:

1. An alleged or suspected violation of the Federal statutes relating to NSI or RD. (10 CFR 95.57(a))

2. An infraction, loss, compromise, or possible compromise of NSI or RD other than actual violations. (10 CFR 95.57(b))

f. Verify that the licensee/certificate holder completes an NRC Form 790 whenever a document containing NSI or RD is generated, has its classi-fication changed, or is declassified; these reports must be forwarded to NRC's Division of Security on a monthly basis. (10 CFR 95.57(c))

02.08 Records. Verify that the licensee/certificate holder keeps the following records and makes them available during security surveys: (10 CFR 95.13)

a. Records of physical checks of security containers made by protective personnel (maintained for 3 years). (10 CFR 95.25(a)(3))

b. Records identifying personnel with knowledge of security container lock combinations (until the list is superseded by a new list or the container is taken out of service). (10 CFR 95.25 (c)(1))

c. Records of lock combinations, marked and protected in a manner appropriate for the highest level applicable. (10 CFR 95.25(d))

d. Records of the date of last change of combinations for all security containers (maintained as long as containers are in service). (10 CFR 95.25(g)(2))

e. Records of unattended security container found open, and actions taken to preclude its recurrence (maintained for 3 years after completion of final corrective action). (10 CFR 95.25(I))

f. Files relating to accountability for keys to gates and doors in the security area (maintained for 3 years after key has been turned in). (10 CFR 95.25(I))

g. Records of employees' security training, refresher training, and termination (maintained for 3 years after termination of employee's access authorization). (10 CFR 95.33)

h. Records of visits and inspections by IAEA representatives, and copies of NRC Division of Security disclosure authorizations for NSI or RD (main-tained for 5 years after the inspection or visit). (10 CFR 95.36(d))

i. Reports of possible unauthorized disclosure of NSI and/or RD due to improper markings or classification are maintained for 3 years after final corrective action has been taken. (10 CFR 95.37(i))

j. Records of disposition for NSI and/or RD material are being maintained for 3 years after the date of disposition. (10 CFR 95.41)

k. Records of destruction for NSI and/or RD material are being maintained for 3 years after the date of destruction. (10 CFR 95.47)

l. Monitor sheets are posted on each security container and that they are being properly utilized. (Retained for 1 month after the sheet is completed). (10 CFR 95.25(g)(3))

81820-03 INSPECTION GUIDANCE

03.01 Security Plan

a. No inspection guidance provided.

b. The accountability procedure for controlling Secret matter should include a log of all Secret matter being retained by the facility, where it is located, who is the custodian, and who has access to it. The procedure should also describe the means by which Secret matter will be destroyed, and should list all Secret documents that have been destroyed.

03.02 Protection of NSI and RD

a-e No inspection guidance provided.

f. A "Q" clearance allows access to material up to Secret and Confidential, both for NSI and RD, whereas an "L" clearance allows access up to Secret NSI but only Confidential RD.

g.

1-2 No inspection guidance provided.

3 When choosing lock combinations, a licensee/certificate holder should avoid obvious numbers to prevent the intruder from guessing the combination. Examples of some obvious numbers to be avoided are simple arithmetic series, birthdays or other dates, license plate numbers and telephone numbers.

4-6 No inspection guidance provided.

h-i No inspection guidance provided.

j. The inspector and licensee/certificate holder should refer to NRC Classification Guide for National Security Information concerning Nuclear Materials and Facilities (CG-NMF-2) for assistance in proper marking of documents.

1-6 No inspection guidance provided.

7 For drafts and working papers that are not transmitted outside the facility, the markings specified in 10 CFR 95.37(c) are not necessary and an NRC Form 790 need not be completed.

8-9 No inspection guidance provided.

k-n No inspection guidance provided.

03.03 Education

a. The security education program should include access authorization requirements, physical security features of the facilities, the classified nature of work, and the classification and sensitivity of the information.

b-c No inspection guidance provided.

03.04 Establishment of Security Areas. No inspection guidance provided.

03.05 Access to NSI and/or RD

a-b No inspection guidance provided.

c. 1-2 No inspection guidance provided.

3 With respect to IAEA, access to NSI is considered relevant to the conduct of the visit/inspection if this information is necessary to verify information submitted pursuant to 10 CFR 75.13 (10 CFR 95.36(b)(1)) or if the information is that to which an inspector would have access under 10 CFR 75.42 (10 CFR 95.36(b)(2)).

03.06 Termination of Facility Approval. Security facility approval will be terminated for reasons of national security or when the licensee/certificate holder no longer has the need for such information. This determination will be confirmed by written notification to the licensee/certificate holder (10 CFR 95.23).

03.07 Notifications and Reports. Notifications of withdrawal or cancellation of security facility approval must identify the facility, the individual requesting the discontinuance, and his/her position with the facility.

81820-04 RESOURCE ESTIMATE

An inspection performed using this inspection procedure is estimated to require 24 hours of inspector resources. This estimate is only for the direct inspection effort and does not include preparation for and documentation of the inspection.

END

1. [1] An "L" clearance is acceptable for access to certain Confidential COMSEC information (see National Communications Security Committee waiver, dated 2/14/84).

PART 95

FACILITY SECURITY CLEARANCE AND SAFEGUARDING OF NATIONAL SECURITY INFORMATION AND RESTRICTED DATA

62 FR 17683

Authority: Secs. 145, 161, 193, 68 Stat. 942, 948, as amended (42 U.S.C. 2165, 2201); sec. 201, 88 Stat. 1242, as amended (42 U.S.C. 5841); E.O. 10865, as amended, 3 CFR 1959–1963 COMP., p. 398 (50 U.S.C. 401, note); E.O. 12829, 3 CFR, 1993 Comp., p. 570; E.O. 12958, as amended, 3 CFR, 1995 Comp., p. 333; E.O. 12968, 3 CFR, 1995 Comp., p. 391.

General Provisions

68 FR 41221

§ 95.1 Purpose.

The regulations in this part establish procedures for obtaining facility security clearance and for safeguarding Secret and Confidential National Security Information and Restricted Data received or developed in conjunction with activities licensed, certified or regulated by the Commission. This part does not apply to Top Secret information because Top Secret information may not be forwarded to licensees, certificate holders, or others within the scope of an NRC license or certificate.

62 FR 17683

§ 95.3 Scope.

The regulations in this part apply to licensees, certificate holders and others regulated by the Commission who may require access to classified National Security Information and/or Restricted Data and/or Formerly Restricted Data (FRD) that is used, processed, stored, reproduced, transmitted, transported, or handled in connection with a license or certificate or an application for a license or certificate.

62 FR 17683

§ 95.5 Definitions.

Access authorization means an administrative determination that an individual (including a consultant) who is employed by or an applicant for employment with the NRC, NRC contractors, agents, licensees and certificate holders, or other person designated by the Executive Director for Operations, is eligible for a security clearance for access to classified information.

45 FR 14476

"Act" means the Atomic Energy Act of 1954 (68 Stat. 919), as amended.

62 FR 17683

Classified mail address means a mail address established for each facility approved by the NRC, to which all classified information for the facility is to be sent.

48 FR 24318

"Classified Matter" means documents or material containing classified information.

62 FR 17683

Classified National Security Information means information that has been determined pursuant to E.O. 12958 or any predecessor order to require protection against unauthorized disclosure and that is so designated.

Classified shipping address means an address established for a facility, approved by the NRC to which classified material that cannot be transmitted as normal mail is to be sent.

Closed area means an area that meets the requirements of the CSA, for the purpose of safeguarding classified material that, because of its size, nature, or operational necessity, cannot be adequately protected by the normal safeguards or stored during nonworking hours in approved containers.

Cognizant Security Agency (CSA) means agencies of the Executive Branch that have been authorized by E.O. 12829 to establish an industrial security program for the purpose of safeguarding classified information under the jurisdiction of those agencies when disclosed or released to U.S. industry. These agencies are the Department of Defense, the Department of Energy, the Central Intelligence Agency, and the Nuclear Regulatory Commission. A facility has a single CSA which exercises primary authority for the protection of classified information at the facility. The CSA for the facility provides security representation for other government agencies with security interests at the facility. The Secretary of Defense has been designated as Executive Agent for the National Industrial Security Program.

45 FR 14476

"Combination Lock" means a three position, manipulation resistant, dial type lock bearing an Underwriters' Laboratories, Inc. certification that it is a Group 1 or Group IR unit.

"Commission" means the Nuclear Regulatory Commission or its duly authorized representatives.

62 FR 17683

Facility (Security) Clearance (FCL) means an administrative determination that, from a security viewpoint, a facility is eligible for access to classified information of a certain category (and all lower categories).

Foreign ownership, control, or influence (FOCI) means a foreign interest has the power, direct or indirect, whether or not exercised, and whether or not exercisable through the ownership of a U.S. company's securities, by contractual arrangements or other means, to direct or decide matters affecting the management or operations of that company in a manner which may result in unauthorized access to classified information or may affect adversely the performance of classified contracts.

Infraction means any knowing, willful, or negligent action contrary to the requirements of E.O. 12958, or its implementing directives, that does not comprise a "violation," as defined in this section.

45 FR 14476

"Intrusion Alarm" means a tamper-indicating electrical, electro-mechanical, electro-optical, electronic or similar device which will detect unauthorized intrusion by an individual into a building, protected area, security area, vital area, or material access area, and alert guards or watchmen by means of actuated visible and audible signals.

[46FR58281]

"License" means a license issued pursuant to 10 CFR Part 50, 70, or 72.

45 FR 14476

"Material" means chemical substance without regard to form; fabricated or processed item; or assembly, machinery or equipment.

"Matter" means documents or material.

48 FR 24318

"National Security" means the national defense or foreign relations of the United States.

62 FR 17683

Need-to-know means a determination made by an authorized holder of classified information that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function under the cognizance of the Commission.

64 FR 15636

NRC "L" access authorization means an access authorization granted by the Commission normally based on a national agency check with law and credit investigation (NACLC) or an access national agency check and inquiries investigation (ANACI)) conducted by the Office of Personnel Management.

NRC "Q" access authorization means an access authorization granted by the Commission normally based on a single scope background investigation conducted by the Office of Personnel Management, the Federal Bureau of Investigation, or other U.S. Government agency that conducts personnel security investigations.

45 FR 14476

"Person" means (1) any individual, corporation, partnership, firm, association, trust, estate, public or private institution, group, government agency other than the Commission or the Department of Energy (DOE), except that the DOE shall be considered a person to the extent that its facilities are subject to the licensing and related regulatory authority of the Commission pursuant to section 202 of the Energy Reorganization Act of 1974 and sections 104, 105 and 202 of the Uranium Mill Tailings Radiation Control Act of 1978, any State or any political subdivision of, or any political entity within a State, any foreign government or nation or any political subdivision of any such government or nation, or other entity; and (2) any legal successor, representative, agent or agency of the foregoing.

"Protective Personnel" means guards or watchmen as defined in 10 CFR Part 73 or other persons designated responsibility for the protection of classified matter.

62 FR 17683

Restricted area means a controlled access area established to safeguard classified material, that because of its size or nature, cannot be adequately protected during working hours by the usual safeguards, but that is capable of being stored during non-working hours in an approved repository or secured by other methods approved by the CSA.

45 FR 14478

"Restricted Data" 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 shall not include data declassified or removed from the Restricted Data category pursuant to Section 142 of the Act.

"Security Area" means a physically defined space containing classified matter and subject to physical protection and personnel access controls.

64 FR 15636

Security container includes any of the following repositories:

(1) A security filing cabinet—one that bears a Test Certification Label on the side of the locking drawer, inside wall adjacent to the locking drawer, or interior door plate, or is marked, "General Services Administration Approved Security Container" on the exterior of the top drawer or door.

(2) A safe—burglar-resistive cabinet or chest which bears a label of the Underwriters' Laboratories, Inc. certifying the unit to be a TL–15, TL–30, or TRTL–30, and has a body fabricated of not less than 1 inch of steel and a door fabricated of not less than 1½ inches of steel exclusive of the combination lock and bolt work; or bears a Test Certification Label on the inside of the door, or is marked "General Services Administration Approved Security Container" and has a body of steel at least ½" thick, and a combination locked steel door at least 1" thick, exclusive of bolt work and locking devices; and an automatic unit locking mechanism.

(3) A vault—a windowless enclosure constructed with walls, floor, roof, and door(s) that will delay penetration sufficient to enable the arrival of emergency response forces capable of preventing theft, diversion, damage, or compromise of classified information or matter, when delay time is assessed in conjunction with detection and communication subsystems of the physical protection system.

(4) A vault-type room—a room that has a combination lock door and is protected by an intrusion alarm system that alarms upon the unauthorized penetration of a person anywhere into the room.

(5) Other repositories that would provide comparable physical protection in the judgment of the Division of Facilities and Security.

45 FR 14476

"Security Facility"—any facility which has been approved by NRC for using, processing, storing, reproducing, transmitting or handling classified matter.

62 FR 17683

Security reviews means aperiodic security reviews of cleared facilities conducted to ensure that safeguards employed by licensees and others are adequate for the protection of classified information.

Supplemental protection means additional security procedures such as intrusion detection systems, security guards, and access control systems.

Violation means any knowing, willful, or negligent action that could reasonably be expected to result in an unauthorized disclosure of classified information or any knowing, willful, or negligent action to classify or continue the classification of information contrary to the requirements of E.O. 12958 or its implementing directives.

45 FR 14476

§ 95.7 Interpretations.

Except as specifically authorized by the Commission in writing, no interpretation of the meaning of the regulations in this part by any officer or employee of the Commission other than a written interpretation by the General Counsel will be recognized to be binding upon the Commission.

62 FR 52184

§ 95.8 Information collection requirements: OMB approval.

(a) The Nuclear Regulatory Commission has submitted the information collection requirements contained in this part to the Office of Management and Budget (OMB) for approval as required by the Paperwork Reduction Act (44 U.S.C. 3501 et seq.). The NRC may not conduct or sponsor, and a person is not required to respond to, a collection of information unless it displays a currently valid OMB control number. OMB has approved the information collection requirements contained in this part under control number 3150–0047.

64 FR 15636

(b) The approved information collection requirements contained in this part appear in §§ 95.11, 95.15, 95.17, 95.18, 95.21, 95.25, 95.33, 95.34, 95.36, 95.37, 95.39, 95.41, 95.43, 95.45, 95.47, 95.53, and 95.57.

68 FR 41221

§ 95.9 Communications.

≫ Except where otherwise specified, all communications and reports concerning the regulations in this part should be addressed to the Director, Division of Nuclear Security, Nuclear Regulatory Commission, Washington, DC 20555.

64 FR 15636

§ 95.11 Specific exemptions.

The NRC may, upon application by any interested person or upon its own initiative, grant exemptions from the requirements of the regulations of this part, that are—

(a) Authorized by law, will not present an undue risk to the public health and safety, and are consistent with the common defense and security; or

(b) Coincidental with one or more of the following:

(1) An application of the regulation in the particular circumstances conflicts with other rules or requirements of the NRC;

(2) An application of the regulation in the particular circumstances would not serve the underlying purpose of the rule or is not necessary to achieve the underlying purpose of the rule;

(3) When compliance would result in undue hardship or other costs that are significantly in excess of those contemplated when the regulation was adopted, or that are significantly in excess of those incurred by others similarly situated;

(4) When the exemption would result in benefit to the common defense and security that compensates for any decrease in security that may result from the grant of the exemption;

(5) When the exemption would provide only temporary relief from the applicable regulation and the licensee or applicant has made good faith efforts to comply with the regulation;

(6) When there is any other material circumstance not considered when the regulation was adopted for which it would be in the public interest to grant an exemption. If such a condition is relied on exclusively for satisfying paragraph (b) of this section, the exemption may not be granted until the Executive Director for Operations has consulted with the Commission.

62 FR 17683

§ 95.13 Maintenance of records.

(a) Each licensee, certificate holder or other person granted facility clearance under this part shall maintain records as prescribed within the part. These records are subject to review and inspection by CSA representatives during security reviews.

53 FR 19240

(b) Each record required by this part must be legible throughout the retention period specified by each Commission regulation. The record may be the original or a reproduced copy or a microform provided that the copy or microform is authenticated by authorized personnel and that the microform is capable of producing a clear copy throughout the required retention period. The record may also be stored in electronic media with the capability for producing legible, accurate, and complete records during the required retention period. Records such as letters, drawings, specifications, must include all pertinent information such as stamps, initials, and signatures. The licensee shall maintain adequate safeguards against tampering with and loss of records.

Physical Security

64 FR 15636

§ 95.15 Approval for processing licensees and others for facility clearance.

(a) A licensee, certificate holder, or other person who has a need to use, process, store, reproduce, transmit, transport, or handle NRC classified information at any location in connection with Commission-related activities shall promptly request an NRC facility clearance. This specifically includes situations where a licensee, certificate holder, or other person needs a contractor or consultant to have access to NRC classified information. Also included are others who require access to classified information in connection with NRC regulated activities but do not require use, storage, or possession of classified information outside of NRC facilities. However, it is not necessary for a licensee, certificate holder, or other person to request an NRC facility clearance for access to another agency's classified information at that agency's facilities or to store that agency's classified information at their facility, provided no NRC classified information is involved and they meet the security requirements of the other agency. If NRC classified information is involved, the requirements of § 95.17 apply.

62 FR 17683

(b) The request must include the name of the facility, the location of the facility and an identification of any facility clearance issued by another government agency. If there is no existing facility clearance, the request must include a security Standard Practice Procedures Plan that outlines the facility's proposed security procedures and controls for the protection of classified information, a floor plan of the area in which the matter is to be used, processed, stored, reproduced, transmitted, transported or handled; and Foreign Ownership, Control or Influence information.

45 FR 14476

(c) NRC will promptly inform applicants of the acceptability of the request for further processing and will notify the licensee or other person of their decision in writing.

95.15(d) [removed] 50 FR 36983

64 FR 15636

§ 95.17 Processing facility clearance.

(a) Following the receipt of an acceptable request for facility clearance, the NRC will either accept an existing facility clearance granted by a current CSA and authorize possession of license or certificate related classified information, or process the facility for a facility clearance. Processing will include—

(1) A determination based on review and approval of a Standard Practice Procedures Plan that granting of the Facility Clearance would not be inconsistent with the national interest, including a finding that the facility is not under foreign ownership, control, or influence to such a degree that a determination could not be made. An NRC finding of foreign ownership, control, or influence is based on factors concerning the foreign intelligence threat, risk of unauthorized technology transfer, type and sensitivity of the information that requires protection, the extent of foreign influence, record of compliance with pertinent laws, and the nature of international security and information exchange agreements. The licensee, certificate holder, or other person must advise the NRC within 30 days of any significant events or changes that may affect its status concerning foreign ownership, control, or influence (e.g., changes in ownership; changes that affect the company's answers to original FOCI questions; indebtedness; and changes in the required form that identifies owners, officers, directors, and executive personnel).

62 FR 17683

(2) An acceptable security review conducted by the NRC;

(3) Submitting key management personnel for personnel clearances (PCLs); and

(4) Appointing a U.S. citizen employee as the facility security officer.

(b) An interim Facility Clearance may be granted by the CSA on a temporary basis pending completion of the full investigative requirements.

62 FR 17683

§ 95.18 Key personnel.

The senior management official and the Facility Security Officer must always be cleared to a level commensurate with the Facility Clearance. Other key management officials, as determined by the CSA, must be granted an access authorization or be excluded from classified access. When formal exclusion action is required, the organization's board of directors or similar executive body shall affirm the following, as appropriate.

(a) Officers, directors, partners, regents, or trustees (designated by name) that are excluded may not require, may not have, and can be effectively excluded from access to all classified information disclosed to the organization. These individuals also may not occupy positions that would enable them to adversely affect the organization's policies or practices in the performance of activities involving classified information. This action will be made a matter of record by the organization's executive body. A copy of the resolution must be furnished to the CSA.

(b) Officers, directors, partners, regents, or trustees (designated by name) that are excluded may not require, may not have, and can be effectively denied access to higher-level classified information (specify which higher level(s)). These individuals may not occupy positions that would enable them to adversely affect the organization's policies or practices in the protection of classified information. This action will be made a matter of record by the organization's executive body. A copy of the resolution must be furnished to the CSA.

68 FR 41221

§ 95.19 Changes to security practices and procedures.

≫ (a) Except as specified in paragraph (b) of this section, each licensee, certificate holder, or other person shall obtain prior CSA approval for any proposed change to the name, location, security procedures and controls, or floor plan of the approved facility. A written description of the proposed change must be furnished to the CSA with copies to the Director, Division of Nuclear Security, Office of Nuclear Security and Incident Response, NRC, Washington, DC 20555–0001 (if NRC is not the CSA), and the NRC Regional Administrator of the cognizant Regional Office listed in appendix A of part 73 of this chapter. These substantive changes to the Standard Practice Procedures Plan that affect the security of the facility must be submitted to the NRC Division of Nuclear Security, or CSA, at least 30 days prior to the change so that they may be evaluated. The CSA shall promptly respond in writing to all such proposals. Some examples of substantive changes requiring prior CSA approval include—

64 FR 15636

(1) A change in the approved facility's classified mail address; or

(2) A temporary or permanent change in the location of the approved facility (e.g., moving or relocating NRC's classified interest from one room or building to another). Approved changes will be reflected in a revised Standard Practice Procedures Plan submission within 30 days of approval. Page changes rather than a complete rewrite of the plan may be submitted.

64 FR 15636

(b) A licensee or other person may effect a minor, non-substantive change to an approved Standard Practice Procedures Plan for the safeguarding of classified information without receiving prior CSA approval. These minor changes that do not affect the security of the facility may be submitted to the addressees noted in paragraph (a) of this section within 30 days of the change. Page changes rather than a complete rewrite of the plan may be submitted. Some examples of minor, non-substantive changes to the Standard Practice Procedures Plan include—

(1) The designation/appointment of a new facility security officer; or

(2) A revision to a protective personnel patrol routine, provided the new routine continues to meet the minimum requirements of this part.

68 FR 41221

≫ (c) A licensee, certificate holder, or other person must update its NRC facility clearance every five years either by submitting a complete Standard Practice Procedures Plan or a certification that the existing plan is fully current to the Division of Nuclear Security.

§ 95.20 Grant, denial or termination of facility clearance.

The Division of Nuclear Security shall provide notification in writing (or orally with written confirmation) to the licensee or other organization of the Commission's grant, acceptance of another agency's facility clearance, denial, or termination of facility clearance. This information must also be furnished to representatives of the NRC, NRC licensees, NRC certificate holders, NRC contractors, or other Federal agencies having a need to transmit classified information to the licensee or other person.

§ 95.21 Withdrawal of requests for facility security clearance.

When a request for facility clearance is to be withdrawn or canceled, the requester shall notify the NRC Division of Nuclear Security in the most expeditious manner so that processing for this approval may be terminated. The notification must identify the full name of the individual requesting discontinuance, his or her position with the facility, and the full identification of the facility. The requestor shall confirm the telephone notification promptly in writing.

62 FR 17683

§ 95.23 Termination of facility clearance.

(a) Facility clearance will be terminated when—

(1) There is no longer a need to use, process, store, reproduce, transmit, transport or handle classified matter at the facility; or

(2) The Commission makes a determination that continued facility clearance is not in the interest of national security.

(b) When facility clearance is terminated, the licensee or other person will be notified in writing of the determination and the procedures outlined in § 95.53 apply.

64 FR 15636

§ 95.25 Protection of National Security Information and Restricted Data in storage.

(a) Secret matter, while unattended or not in actual use, must be stored in—

62 FR 17683

(1) A safe, steel file cabinet, or safe-type steel file container that has an automatic unit locking mechanism. All such receptacles will be accorded supplemental protection during non-working hours; or

64 FR 15636

(2) Any steel file cabinet that has four sides and a top and bottom (all permanently attached by welding, rivets, or peened bolts so the contents cannot be removed without leaving visible evidence of entry) and is secured by a rigid metal lock bar and an approved key operated or combination padlock. The keepers of the rigid metal lock bar must be secured to the cabinet by welding, rivets, or bolts, so they cannot be removed and replaced without leaving evidence of the entry. The drawers of the container must be held securely so their contents cannot be removed without forcing open the drawer. This type of cabinet will be accorded supplemental protection during non-working hours.

(b) Confidential matter while unattended or not in use must be stored in the same manner as SECRET matter except that no supplemental protection is required.

62 FR 17683

(c) Classified lock combinations.

(1) A minimum number of authorized persons may know the combinations to authorized storage containers. Security containers, vaults, cabinets, and other authorized storage containers must be kept locked when not under the direct supervision of an authorized person entrusted with the contents.

64 FR 15636

(2) Combinations must be changed by a person authorized access to the contents of the container, by the Facility Security Officer, or his or her designee.

62 FR 17683

(d) Records of combinations. If a record is made of a combination, the record must be marked with the highest classification of material authorized for storage in the container. Superseded combinations must be destroyed.

45 FR 14476

(e) Selections of combinations: Each combination must be randomly selected and require the use of at least three different numbers. In selecting combinations, multiples, simple arithmetical ascending or descending series, telephone numbers, social security numbers, car license numbers, and calendar dates such as birthdates and anniversaries, shall be avoided.

64 FR 15636

(f) Combinations will be changed only by persons authorized access to Secret or Confidential National Security Information and/or Restricted Data depending upon the matter authorized to be stored in the security container.

(g) Posted information. Containers may not bear external markings indicating the level of classified matter authorized for storage. A record of the names of persons having knowledge of the combination must be posted inside the container.

(h) End of day security checks.

(1) Facilities that store classified matter shall establish a system of security checks at the close of each working day to ensure that all classified matter and security repositories have been appropriately secured.

(2) Facilities operating with multiple work shifts shall perform the security checks at the end of the last working shift in which classified matter had been removed from storage for use. The checks are not required during continuous 24-hour operations.

(i) Unattended security container found opened. If an unattended security container housing classified matter is found unlocked, the custodian or an alternate must be notified immediately. Also, the container must be secured by protective personnel. An effort must be made to determine if the contents were compromised not later than the next day.

62 FR 17683

(j) Supervision of keys and padlocks. Use of key-operated padlocks are subject to the following requirements:

64 FR 15636

(1) A key and lock custodian shall be appointed to ensure proper custody and handling of keys and locks used for protection of classified matter;

62 FR 17683

(2) A key and lock control register must be maintained to identify keys for each lock and their current location and custody;

(3) Keys and locks must be audited each month;

(4) Keys must be inventoried with each change of custody;

(5) Keys must not be removed from the premises;

64 FR 15636

(6) Keys and spare locks must be protected equivalent to the level of classified matter involved;

(7) Locks must be changed or rotated at least every 12 months, and must be replaced after loss or compromise of their operable keys; and

62 FR 17683

(8) Master keys may not be made.

64 FR 15636

§ 95.27 Protection while in use.

While in use, classified matter must be under the direct control of an authorized individual to preclude physical, audio, and visual access by persons who do not have the prescribed access authorization or other written CSA disclosure authorization (see § 95.36 for additional information concerning disclosure authorizations).

§ 95.29 Establishment of restricted or closed areas.

(a) If, because of its nature, sensitivity or importance, classified matter cannot otherwise be effectively controlled in accordance with the provisions of §§ 95.25 and 95.27, a Restricted or Closed area must be established to protect this matter.

62 FR 17683

(b) The following measures apply to Restricted Areas:

(1) Restricted areas must be separated from adjacent areas by a physical barrier designed to prevent unauthorized access (physical, audio, and visual) into these areas.

(2) Controls must be established to prevent unauthorized access to and removal of classified matter.

(3) Access to classified matter must be limited to persons who possess appropriate access authorization or other written CSA disclosure authorization and who require access in the performance of their official duties or regulatory obligations.

(4) Persons without appropriate access authorization for the area visited must be escorted by an appropriate CSA access authorized person at all times while within Restricted or Closed Areas.

(5) Each individual authorized to enter a Restricted or Closed Area must be issued a distinctive form of identification (e.g., badge) when the number of employees assigned to the area exceeds thirty per shift.

(6) During nonworking hours, admittance must be controlled by protective personnel. Protective personnel shall conduct patrols during nonworking hours at least every 8 hours and more frequently if necessary to maintain a commensurate level of protection. Entrances must be continuously monitored by protective personnel or by an approved alarm system.

(c) Due to the size and nature of the classified material, or operational necessity, it may be necessary to construct Closed Areas for storage because GSA-approved containers or vaults are unsuitable or impractical. Closed Areas must be approved by the CSA. The following measures apply to Closed Areas:

(1) Access to Closed Areas must be controlled to preclude unauthorized access. This may be accomplished through the use of a cleared employee or by a CSA approved access control device or system.

64 FR 15636

(2) Access must be limited to authorized persons who have an appropriate security clearance and a need-to-know for the classified matter within the area. Persons without the appropriate level of clearance and/or need-to-know must be escorted at all times by an authorized person where inadvertent or unauthorized exposure to classified information cannot otherwise be effectively prevented.

62 FR 17683

(3) The Closed Area must be accorded supplemental protection during non-working hours. During these hours, admittance to the area must be controlled by locked entrances and exits secured by either an approved built-in combination lock or an approved combination or key-operated padlock. However, doors secured from the inside with a panic bolt (for example, actuated by a panic bar), a dead bolt, a rigid wood or metal bar, or other means approved by the CSA, do not require additional locking devices.

64 FR 15636

(4) Open shelf or bin storage of classified matter in Closed Areas requires CSA approval. Only areas protected by an approved intrusion detection system will qualify for approval.

62 FR 17683

§ 95.31 Protective personnel.

Whenever protective personnel are used to protect classified information they shall:

(a) Possess an "L" access authorization (or CSA equivalent) if the licensee or other person possesses information classified Confidential National Security Information, Confidential Restricted Data or Secret National Security Information.

(b) Possess a "Q" access authorization (or CSA equivalent) if the licensee or other person possesses Secret Restricted Data related to nuclear weapons design, manufacturing and vulnerability information; and certain particularly sensitive Naval Nuclear Propulsion Program information (e.g., fuel manufacturing technology) and the protective personnel require access as part of their regular duties.

§ 95.33 Security education.

All cleared employees must be provided with security training and briefings commensurate with their involvement with classified information. The facility may obtain defensive security, threat awareness, and other education and training information and material from their CSA or other sources.

(a) Facility Security Officer Training. Licensees and others are responsible for ensuring that the Facility Security Officer, and others performing security duties, complete security training deemed appropriate by the CSA. Training requirements must be based on the facility's involvement with classified information and may include a Facility Security Officer orientation course and, for Facility Security Officers at facilities with safeguarding capability, a Facility Security Officer Program Management Course. Training, if required, should be completed within 1 year of appointment to the position of Facility Security Officer. 62 FR 17683

(b) Government-Provided Briefings. The CSA is responsible for providing initial security briefings to the Facility Security Officer, and for ensuring that other briefings required for special categories of information are provided.

(c) Temporary Help Suppliers. A temporary help supplier, or other contractor who employs cleared individuals solely for dispatch elsewhere, is responsible for ensuring that required briefings are provided to their cleared personnel. The temporary help supplier or the using licensee or other facility may conduct these briefings.

(d) Classified Information Nondisclosure Agreement (SF–312). The SF–312 is an agreement between the United States and an individual who is cleared for access to classified information. An employee issued an initial access authorization must, in accordance with the requirements of § 25.23 of this chapter, execute an SF–312 before being granted access to classified information. The Facility Security Officer shall forward the executed SF–312 to the CSA for retention. If the employee refuses to execute the SF–312, the licensee or other facility shall deny the employee access to classified information and submit a report to the CSA. The SF–312 must be signed and dated by the employee and witnessed. The employee's and witness' signatures must bear the same date. 62 FR 17683

(e) Initial Security Briefings. Before being granted access to classified information, an employee shall receive an initial security briefing that includes the following topics:

(1) A Threat Awareness Briefing.

(2) A Defensive Security Briefing.

(3) An overview of the security classification system.

(4) Employee reporting obligations and requirements.

(5) Security procedures and duties applicable to the employee's job.

(f) Refresher Briefings. The licensee or other facility shall conduct refresher briefings for all cleared employees every 3 years. As a minimum, the refresher briefing must reinforce the information provided during the initial briefing and inform employees of appropriate changes in security regulations. This requirement may be satisfied by use of audio/video materials and/or by issuing written materials. 64 FR 15636

(g) Debriefings. Licensee and other facilities shall debrief cleared employees at the time of termination of employment (discharge, resignation, or retirement); when an employee's access authorization is terminated, suspended, or revoked; and upon termination of the Facility Clearance. 62 FR 17683

(h) Records reflecting an individual's initial and refresher security orientations and security termination must be maintained for three years after termination of the individual's access authorization.

Control of Information

64 FR 15636

§ 95.34 Control of visitors.

(a) *Uncleared visitors.* Licensees, certificate holders, or others subject to this part shall take measures to preclude access to classified information by uncleared visitors.

(b) *Foreign visitors.* Licensees, certificate holders, or others subject to this part shall take measures as may be necessary to preclude access to classified information by foreign visitors. The licensee, certificate holder, or others shall retain records of visits for 5 years beyond the date of the visit.

59 FR 48944

§ 95.35 Access to matter classified as National Security Information and Restricted Data.

(a) Except as the Commission may authorize, no person subject to the regulations in this part may receive or may permit any individual to have access to matter revealing Secret or Confidential National Security Information or Restricted Data unless the individual has:

(1)(i) A "Q" access authorization which permits access to matter classified as Secret and Confidential Restricted Data or Secret and Confidential National Security Information which includes intelligence information, CRYPTO (i.e., cryptographic information) or other classified communications security (COMSEC) information, or

(ii) An "L" access authorization which permits access to matter classified as Confidential Restricted Data and Secret and Confidential National Security Information other than that noted in paragraph (a)(1)(i) of this section except that access to certain Confidential COMSEC information is permitted as authorized by a National Communications Security Committee waiver dated February 14, 1984.

(2) An established "need-to-know" for the matter (See Definitions, § 95.5).

(3) NRC-approved storage facilities if classified documents or material are to be transmitted to the individual.

(b) Matter classified as National Security Information or Restricted Data shall not be released by a licensee or other person subject to part 95 to any personnel other than properly access authorized Commission licensee employees, or other individuals authorized access by the Commission.

(c) Access to matter which is National Security Information at NRC-licensed facilities or NRC-certified facilities by authorized representatives of IAEA is permitted in accordance with § 95.36.

68 FR 41221

§ 95.36 Access by representatives of the International Atomic Energy Agency or by participants in other international agreements.

≫ (a) Based upon written disclosure authorization from the NRC Division of Nuclear Security that an individual is an authorized representative of the International Atomic Energy Agency (IAEA) or other international organization and that the individual is authorized to make visits or inspections in accordance with an established agreement with the United States Government, a licensee, certificate holder, or other person subject to this part shall permit the individual (upon presentation of the credentials specified in § 75.7 of this chapter and any other credentials identified in the disclosure authorization) to have access to matter classified as National Security Information that is relevant to the conduct of a visit or inspection. A disclosure authorization under this section does not authorize a licensee, certificate holder, or other person subject to this part to provide access to Restricted Data.

62 FR 17683

(b) For purposes of this section, classified National Security Information is relevant to the conduct of a visit or inspection if—

(1) In the case of a visit, this information is needed to verify information according to § 75.13 of this chapter; or

(2) In the case of an inspection, an inspector is entitled to have access to the information under § 75.42 of this chapter.

68 FR 41221

≫ (c) In accordance with the specific disclosure authorization provided by the Division of Nuclear Security, licensees or other persons subject to this part are authorized to release (i.e., transfer possession of) copies of documents that contain classified National Security Information directly to IAEA inspectors and other representatives officially designated to request and receive classified National Security Information documents. These documents must be marked specifically for release to IAEA or other international organizations in accordance with instructions contained in the NRC's disclosure authorization letter. Licensees and other persons subject to this part may also forward these documents through the NRC to the international organization's headquarters in accordance with the NRC disclosure authorization. Licensees and other persons may not reproduce documents containing classified National Security Information except as provided in § 95.43.

(d) Records regarding these visits and inspections must be maintained for 5 years beyond the date of the visit or inspection. These records must specifically identify each document released to an authorized representative and indicate the date of the release. These records must also identify (in such detail as the Division of Nuclear Security, by letter, may require) the categories of documents that the authorized representative has had access and the date of this access. A licensee or other person subject to this part shall also retain Division of Nuclear Security disclosure authorizations for 5 years beyond the date of any visit or inspection when access to classified information was permitted.

62 FR 17683

(e) Licensees or other persons subject to this part shall take such measures as may be necessary to preclude access to classified matter by participants of other international agreements unless specifically provided for under the terms of a specific agreement.

§ 95.37 Classification and preparation of documents.

(a) Classification. Classified information generated or possessed by a licensee or other person must be appropriately marked. Classified material which is not conducive to markings (e.g., equipment) may be exempt from this requirement. These exemptions are subject to the approval of the CSA on a case-by-case basis. If a person or facility generates or possesses information that is believed to be classified based on guidance provided by the NRC or by derivation from classified documents, but which no authorized classifier has determined to be classified, the information must be protected and marked with the appropriate classification markings pending review and signature of an NRC authorized classifier. This information shall be protected as classified information pending final determination.

(b) Classification consistent with content. Each document containing classified information shall be classified Secret or Confidential according to its content. NRC licensees or others subject to the requirements of 10 CFR Part 95 may not make original classification decisions.

(c) Markings required on face of documents.

(1) For derivative classification of classified National Security Information:

64 FR 15636

(i) Derivative classifications of classified National Security Information must contain the identity of the source document or the classification guide, including the agency and office of origin, on the "Derived From" line and its classification date. If more than one source is cited, the "Derived From" line should indicate "Multiple Sources." The derivative classifier shall maintain the identification of each source with the file or record copy of the derivatively classified document.

62 FR 17683

(ii) Declassification instructions. When marking derivatively classified documents, the "DECLASSIFY ON" line must carry forward the declassification instructions as reflected in the original document. If multiple sources are used, the instructions will carry forward the longest duration.

68 FR 41221

(iii) An example of the marking stamp is as follows:

Derived from _____
(Source/Date)

Reason: _____

Declassify On: _____
(Date/Event/Exemption)

Classifier: _____
(Name/Title/Number)

(iv) [Removed 64 FR 15636.]

62 FR 17683

(2) For Restricted Data documents:

(i) Identity of the classifier. The identity of the classifier must be shown by completion of the "Derivative Classifier" line. The "Derivative Classifier" line must show the name of the person classifying the document and the basis for the classification. Dates for downgrading or declassification do not apply.

(ii) Classification designation (e.g., Secret, Confidential) and Restricted Data. NOTE: No "Declassification" instructions will be placed on documents containing Restricted Data.

(d) Placement of markings. The highest classification marking assigned to a document must be placed in a conspicuous fashion in letters at the top and bottom of the outside of the front covers and title pages, if any, and first and last pages on which text appears, on both bound and unbound documents, and on the outside of back covers of bound documents. The balance of the pages must be marked at the top and bottom with:

(1) The overall classification marking assigned to the document;

(2) The highest classification marking required by content of the page; or

(3) The marking UNCLASSIFIED if they have no classified content.

(e) Additional markings.

(1) If the document contains any form of Restricted Data, it must bear the appropriate marking on the first page of text, on the front cover and title page, if any. For example: "This document contains Restricted Data as defined in the Atomic Energy Act of 1954. Unauthorized disclosure subject to Administrative and Criminal Sanctions."

(2) Limitation on reproduction or dissemination. If the originator or classifier determines that reproduction or further dissemination of a document should be restricted, the following additional wording may be placed on the face of the document:

Reproduction or Further Dissemination Requires Approval of

_____

If any portion of this additional marking does not apply, it should be crossed out.

(f) Portion markings. In addition to the information required on the face of the document, each classified document is required, by marking or other means, to indicate clearly which portions are classified (e.g., paragraphs or pages) and which portions are not classified. The symbols (S) for Secret, (C) for Confidential, (U) for Unclassified, or (RD) for Restricted Data may be used immediately preceding or following the text to which it applies, except that the designation must follow titles or subjects. (Portion marking of paragraphs is not required for documents containing Restricted Data.) If this type of portion marking is not practicable, the document must contain a description sufficient to identify the classified information and the unclassified information.

Example

Pages 1–3 Secret
Pages 4–19 Unclassified
Pages 20–26 Secret
Pages 27–32 Confidential

62 FR 17683

(g) Transmittal document. If a document transmitting classified information contains no classified information or the classification level of the transmittal document is not as high as the highest classification level of its enclosures, then the document must be marked at the top and bottom with a classification at least as high as its highest classified enclosure. The classification may be higher if the enclosures, when combined, warrant a higher classification than any individual enclosure. When the contents of the transmittal document warrants a lower classification than the highest classified enclosure(s) or combination of enclosures or requires no classification, a stamp or marking such as the following must also be used on the transmittal document:

UPON REMOVAL OF ATTACHMENTS THIS DOCUMENT IS:
(Classification level of transmittal document standing alone or the word "UNCLASSIFIED" if the transmittal document contains no classified information.)

(h) Classification challenges. Persons in authorized possession of classified National Security Information who in good faith believe that the information's classification status (i.e. that the document), is classified at either too high a level for its content (overclassification) or too low for its content (underclassification) are expected to challenge its classification status. Persons who wish to challenge a classification status shall—

62 FR 17683

(1) Refer the document or information to the originator or to an authorized NRC classifier for review. The authorized classifier shall review the document and render a written classification decision to the holder of the information.

64 FR 15636

(2) In the event of a question regarding classification review, the holder of the information or the authorized classifier shall consult the NRC Division of Facilities and Security, Information Security Branch, for assistance.

62 FR 17683

(3) Persons who challenge classification decisions have the right to appeal the classification decision to the Interagency Security Classification Appeals Panel.

(4) Persons seeking to challenge the classification of information will not be the subject of retribution.

(i) Files, folders or group of documents. Files, folders, binders, or groups of physically connected documents must be marked at least as high as the highest classified document which they contain.

(j) Drafts and working papers. Drafts of documents and working papers which contain, or which are believed to contain, classified information must be marked as classified information.

(k) Classification guidance. Licensees, certificate holders, or other persons subject to this part shall classify and mark classified matter as National Security Information or Restricted Data, as appropriate, in accordance with classification guidance provided by the NRC as part of the facility clearance process.

64 FR 15636

§ 95.39 External transmission of classified matter.

62 FR 17683

(a) Restrictions. Documents and material containing classified information received or originated in connection with an NRC license or certificate must be transmitted only to CSA approved security facilities.

(b) Preparation of documents. Documents containing classified information must be prepared in accordance with the following when transmitted outside an individual installation.

(1) The documents must be enclosed in two sealed opaque envelopes or wrappers.

(2) The inner envelope or wrapper must contain the addressee's classified mail address and the name of the intended recipient. The appropriate classification must be placed on both sides of the envelope (top and bottom) and the additional markings, as appropriate, referred to in § 95.37(e) must be placed on the side bearing the address.

64 FR 15636

(3) The outer envelope or wrapper must contain the addressee's classified mailing address. The outer envelope or wrapper may not contain any classification, additional marking or other notation that indicate that the enclosed document contains classified information. The Classified Mailing Address shall be uniquely designated for the receipt of classified information. The classified shipping address for the receipt of material (e.g., equipment) should be different from the classified mailing address for the receipt of classified documents.

62 FR 17683

(4) A receipt that contains an unclassified description of the document, the document number, if any, date of the document, classification, the date of transfer, the recipient and the person transferring the document must be enclosed within the inner envelope containing the document and be signed by the recipient and returned to the sender whenever the custody of a Secret document is transferred. This receipt process is at the option of the sender for Confidential information.

(c) Methods of transportation.

(1) Secret matter may be transported only by one of the following methods within and directly between the U.S., Puerto Rico, or a U.S. possession or trust territory:

(i) U.S. Postal Service Express Mail and U.S. Postal Service Registered Mail.

Note: The "Waiver of Signature and Indemnity" block on the U.S. Postal Service Express Mail Label 11–B may not be executed and the use of external (street side) express mail collection boxes is prohibited.

(ii) A cleared "Commercial Carrier."

(iii) A cleared commercial messenger service engaged in the intracity/local area delivery (same day delivery only) of classified material.

(iv) A commercial delivery company, approved by the CSA, that provides nationwide, overnight service with computer tracing and reporting features. These companies need not be security cleared.

(v) Other methods as directed, in writing, by the CSA.

64 FR 15636

(2) Confidential matter may be transported by one of the methods set forth in paragraph (c)(1) of this section, by U.S. express or certified mail. Express or certified mail may be used in transmission of Confidential documents to Puerto Rico or any United States territory or possession.

62 FR 17683

(d) Telecommunication of classified information. Classified information may not be telecommunicated unless the telecommunication system has been approved by the CSA. Licensees, certificate holders or other persons who may require a secure telecommunication system shall submit a telecommunication plan as part of their request for facility clearance, as outlined in § 95.15, or as an amendment to their existing Standard Practice Procedures Plan for the protection of classified information.

(e) Security of classified information in transit. Classified matter that, because of its nature, cannot be transported in accordance with § 95.39(c), may only be transported in accordance with procedures approved by the CSA. Procedures for transporting classified matter are based on a satisfactory transportation plan submitted as part of the licensee's, certificate holder, or other person's request for facility clearance or submitted as an amendment to its existing Standard Practice Procedures Plan.

§ 95.41 External receipt and dispatch records.

Each licensee, certificate holder or other person possessing classified information shall maintain a record that reflects:

(a) The date of the material;

(b) The date of receipt or dispatch;

(c) The classification;

(d) An unclassified description of the material; and

(e) The identity of the sender from which the material was received or recipient to which the material was dispatched. Receipt and dispatch records must be retained for 2 years.

§ 95.43 Authority to reproduce.

(a) Each licensee or other person possessing classified information shall establish a reproduction control system to ensure that reproduction of classified material is held to the minimum consistent with operational requirements. Classified reproduction must be accomplished by authorized employees knowledgeable of the procedures for classified reproduction. The use of technology that prevents, discourages, or detects the unauthorized reproduction of classified documents is encouraged.

(b) Unless restricted by the CSA, Secret and Confidential documents may be reproduced. Reproduced copies of classified documents are subject to the same protection as the original documents.

(c) All reproductions of classified material must be conspicuously marked with the same classification markings as the material being reproduced. Copies of classified material must be reviewed after the reproduction process to ensure that these markings are visible.

62 FR 17683

§ 95.45 Changes in classification.

(a) Documents containing classified National Security Information must be downgraded or declassified as authorized by the NRC classification guides or as determined by the NRC. Requests for downgrading or declassifying any NRC classified information should be forwarded to the NRC Division of Nuclear Security, Office of Nuclear Security and Incident Response, Washington, DC 20555–0001. Requests for downgrading or declassifying of Restricted Data will be forwarded to the NRC Division of Nuclear Security for coordination with the Department of Energy.

68 FR 41221

(b) If a change of classification or declassification is approved, the previous classification marking must be canceled and the following statement, properly completed, must be placed on the first page of the document:

Classification canceled (or changed to)

_____

(Insert appropriate classification)

By authority of

_____

(Person authorizing change in classification)

By

_____

(Signature of person making change and date thereof)

(c) New markings reflecting the current classification status of the document will be applied in accordance with the requirements of § 95.37.

(d) Any persons making a change in classification or receiving notice of such a change shall forward notice of the change in classification to holders of all copies as shown on their records.

62 FR 17683

§ 95.47 Destruction of matter containing classified information.

Documents containing classified information may be destroyed by burning, pulping, or another method that ensures complete destruction of the information that they contain. The method of destruction must preclude recognition or reconstruction of the classified information. Any doubts on methods should be referred to the CSA.

64 FR 15636

62 FR 17683

§ 95.49 Security of automatic data processing (ADP) systems.

Classified data or information may not be processed or produced on an ADP system unless the system and procedures to protect the classified data or information have been approved by the CSA. Approval of the ADP system and procedures is based on a satisfactory ADP security proposal submitted as part of the licensee's or other person's request for facility clearance outlined in § 95.15 or submitted as an amendment to its existing Standard Practice Procedures Plan for the protection of classified information.

§ 95.51 Retrieval of classified matter following suspension or revocation of access authorization.

In any case where the access authorization of an individual is suspended or revoked in accordance with the procedures set forth in part 25 of this chapter, or other relevant CSA procedures, the licensee, certificate holder or other organization shall, upon due notice from the Commission of such suspension or revocation, retrieve all classified information possessed by the individual and take the action necessary to preclude that individual having further access to the information.

68 FR 41221

§ 95.53 Termination of facility clearance.

≫(a) If the need to use, process, store, reproduce, transmit, transport, or handle classified matter no longer exists, the facility clearance will be terminated. The facility may deliver all documents and matter containing classified information to the Commission, or to a person authorized to receive them, or must destroy all classified documents and matter. In either case, the facility shall submit a certification of nonpossession of classified information to the NRC Division of Nuclear Security within 30 days of the termination of the facility clearance.

64 FR 15636

(b) In any instance where a facility clearance has been terminated based on a determination of the CSA that further possession of classified matter by the facility would not be in the interest of the national security, the facility shall, upon notice from the CSA, dispose of classified documents in a manner specified by the CSA.

62 FR 17683

§ 95.55 Continued applicability of the regulations in this part.

The suspension, revocation or other termination of access authorization or the termination of facility clearance does not relieve any person from compliance with the regulations in this part.

64 FR 15636

§ 95.57 Reports.

Each licensee or other person having a facility clearance shall report to the CSA and the Regional Administrator of the appropriate NRC Regional Office listed in 10 CFR part 73, appendix A:

(a) Any alleged or suspected violation of the Atomic Energy Act, Espionage Act, or other Federal statutes related to classified information (e.g., deliberate disclosure of classified information to persons not authorized to receive it, theft of classified information). Incidents such as this must be reported within 1 hour of the event followed by written confirmation within 30 days of the incident; and

(b) Any infractions, losses, compromises, or possible compromise of classified information or classified documents not falling within paragraph (a) of this section. Incidents such as these must be entered into a written log. A copy of the log must be provided to the NRC on a monthly basis. Details of security infractions including corrective action taken must be available to the CSA upon request.

68 FR 41221

≫(c) In addition, NRC requires records for all classification actions (documents classified, declassified, or downgraded) to be submitted to the NRC Division of Nuclear Security. These may be submitted either on an "as completed" basis or monthly. The information may be submitted either electronically by an on-line system (NRC prefers the use of a dial-in automated system connected to the Division of Nuclear Security) or by paper copy using NRC Form 790.

62 FR 17683

§ 95.59 Inspections.

The Commission shall make inspections and reviews of the premises, activities, records and procedures of any person subject to the regulations in this part as the Commission and CSA deem necessary to effect the purposes of the Act, E.O. 12958 and/or NRC rules.

Violations

57 FR 55062

§ 95.61 Violations.

(a) The Commission may obtain an injunction or other court order to prevent a violation of the provisions of—

(1) The Atomic Energy Act of 1954, as amended;

(2) Title II of the Energy Reorganization Act of 1974, as amended; or

(3) A regulation or order issued pursuant to those Acts.

(b) The Commission may obtain a court order for the payment of a civil penalty imposed under section 234 of the Atomic Energy Act:

(1) For violations of—

(i) Sections 53, 57, 62, 63, 81, 82, 101, 103, 104, 107, or 109 of the Atomic Energy Act of 1954, as amended;

(ii) Section 206 of the Energy Reorganization Act;

(iii) Any rule, regulation, or order issued pursuant to the sections specified in paragraph (b)(1)(i) of this section;

(iv) Any term, condition, or limitation of any license issued under the sections specified in paragraph (b)(1)(i) of this section.

(2) For any violation for which a license may be revoked under Section 186 of the Atomic Energy Act of 1954, as amended.

§ 95.63 Criminal penalties.

(a) Section 223 of the Atomic Energy Act of 1954, as amended, provides for criminal sanctions for willful violation of, attempted violation of, or conspiracy to violate, any regulation issued under sections 161b, 161i, or 161o of the Act. For purposes of section 223, all the regulations in part 95 are issued under one or more of sections 161b, 161i, or 161o, except for the sections listed in paragraph (b) of this section.

(b) The regulations in part 95 that are not issued under sections 161b, 161i, or 161o for the purposes of section 223 are as follows: §§ 95.1, 95.3, 95.5, 95.7, 95.8, 95.9, 95.11, 95.17, 95.19, 95.21, 95.23, 95.55, 95.59, 95.61, and 95.63.

Appendix A to Part 95
[Removed 59 FR 48944.]

Standard Practice Procedures Plan
Standard Format And Content For The Protection of Classified Matter For NRC Licensee, Certificate Holder, And Others Regulated by the Commission

Division of Facilities and Security
U. S. Nuclear Regulatory Commission

October 1999

FOREWORD

The attached Format and Content Guide is designed to assist in the preparation of a Standard Practice Procedures Plan that outlines the specific security procedures and controls that have been implemented at Nuclear Regulatory Commission (NRC) licensed, certified or regulated facilities for the protection of classified matter. It is a living document that will be modified or improved based on user feedback and as a result of ongoing and future policy, and guidance initiatives.

Questions or suggestions regarding this format and content guide should be directed to NRC's Division of Facilities and Security at (301) 415-7048.

TABLE OF CONTENTS

STANDARD PRACTICE PROCEDURES PLAN
STANDARD FORMAT AND CONTENT FOR THE PROTECTION OF CLASSIFIED MATTER FOR NUCLEAR REGULATORY COMMISSION LICENSEE, CERTIFICATE HOLDER, AND OTHERS REGULATED BY THE COMMISSION

1.0 PURPOSE

The regulations in 10 CFR 25 and 95 establish procedures for the following:

Granting, reinstating, extending, transferring, and terminating access authorizations of licensee personnel, licensee contractors or agents, and other persons (e.g., individuals involved in adjudicatory procedures as set forth in 10 CFR Part 2, subpart I) who may require access to classified information. (10 CFR 25.1)

Obtaining a Facility Security Clearance and for safeguarding SECRET and CONFIDENTIAL National Security Information (NSI) and Restricted Data (RD) received or developed in conjunction with activities licensed, certified or regulated by the Commission. This section does not apply to TOP SECRET information because TOP SECRET information may not be forwarded to licensees, certificate holders, or others within the scope of a Nuclear Regulatory Commission (NRC) license or certificate. (10 CFR 95.1)

2.0 SCOPE

The regulations in 10 CFR 25 and 95 apply to:

Licensees and others who may require access to classified information related to a license or an application for a license. (10 CFR 25.3)

Licensees, certificate holders and others regulated by the Commission who may require access to classified NSI, RD, and/or Formerly Restricted Data (FRD) that is used, processed, stored, reproduced, transmitted, transported, or handled in connection with a license or certificate or an application for a license or certificate. (10 CFR 95.3)

3.0 SITE AND FACILITY DESCRIPTION (10 CFR 95.15 (b))

3.1 Facility Name and Address

Name the licensee, certificate holder, or others. Include the division or department, if applicable. Identify the precise street, address, or location to differentiate the facility from other buildings or groups of buildings not related to the request for Facility Security Clearance approval.

Example: Ott Nuclear Company, Inc.
Nuclear Manufacturing Division
806 Bradford Street
San Francisco, California 94110

3.2 Description of Site and Identification of Activity

Describe the site on which the building or buildings are located where NRC classified matter will be used, processed, stored, reproduced, transmitted, transported, or otherwise handled. Include a statement of the nature of the NRC activity at the site.

Describe the general character of the location (e.g., rural, suburban, or urban), distance to the nearest city or town, outer perimeter security (e.g., fences or guard stations), and the physical proximity to other buildings.

3.3 Security Storage Facility

3.3.1 Location of Classified Matter

Identify the specific locations (e.g., on a floor plan and by building) where NRC classified matter will be used, processed, stored, reproduced, transmitted, transported, or otherwise handled.

3.3.2 Construction Features

Describe the type of building construction (e.g., brick, cinder block, or steel) and the location of walls, windows, doors, and the openings in the building(s) or portions of building used as barriers where NRC classified matter will be used, processed, etc. Provide scaled drawings showing these features. Describe the type, make and model of the storage container in which the classified material will be secured when not in use.

3.4 Classified Mail/Shipping Address

Furnish the address, including Zip Code, at which classified mail and matter (other than mail) will be received. If classified mail and matter are received at different addresses, include both addresses. Also include an "Attention" line for the inner envelope or package showing the recipient who is cleared and authorized to receive classified matter. If applicable, identify the precise recipient, street, address, or location where classified matter (other than mail) is to be delivered.

3.5 Foreign Ownership, Control or Influence (FOCI)

It is the policy of the U.S. Government to allow foreign investment consistent with the national security interests of the United States.

NRC's policy concerning the initial or continued clearance eligibility of U.S. companies with foreign involvement includes providing criteria for determining whether U.S. companies are under FOCI; prescribes responsibilities in FOCI matters; and outlines security measures that may be considered to negate or reduce to an acceptable level FOCI-based security risks. The foreign involvement of U.S. companies cleared or under consideration for a Facility Security Clearance (FCL) is examined to ensure appropriate resolution of matters determined to be of national security significance. The development of security measures to negate FOCI determined to be unacceptable shall be based on the concept of risk management. The determination of whether a U.S. company is under FOCI, its eligibility for an FCL, and the security measures deemed necessary to negate FOCI shall be made on a case-by-case basis. (10 CFR 95.17)(NISPOM Ch. 2, Sect. 3)

Describe the procedures in place to ensure that the licensee, certificate holder, or other person is free from foreign ownership, control, or influence to the extent that it could result in the compromise of classified information/matter. This procedure should include all contractors and subcontractors handling classified information/matter for the licensee, certificate holder, or other person.

3.6 Key Personnel

Identify the clearance levels of Key Management personnel to include the senior management official and the Facility Security Officer (FSO) to ensure that they are cleared to the level commensurate with the Facility Security Clearance. Also, describe any resolutions that exclude officers, directors, partners, regents, or trustees from access to classified information disclosed to the organization. (10 CFR 95.18(a & b)

3.7 Other Agencies Approved Plans

Identify and provide copies of any Security Plan (e.g., ADP) approved by other Federal agencies.

4.0 SECURITY ORGANIZATION

Describe the person and/or organization responsible for the security of classified matter at the facility. Describe the responsibilities and the relationship of the security organization dealing with classified matter to the overall management of the concern. Include a description of the security responsibilities for each organizational entity within the security organization responsible for NRC classified matter. Indicate the

chain of command for decision-making on matters affecting the security of classified matter. Identify the FSO and at least one alternate responsible for the security of classified matter.

5.0 TYPE OF CLASSIFIED INFORMATION/MATTER

5.1 Type of Classified Information/Matter To Be Handled

Determine whether National Security Information, Restricted Data, Communications Security (COMSEC) Information, or other types of information/matter will be used, processed, stored, reproduced, transmitted, transported, or otherwise handled by the licensee, certificate holder or related organization. Identify the nature (documents or material) and the highest level of classification of the matter expected to be involved.

5.2 Description of Classified Information/Matter

Describe, in as specific terms as possible, the exact nature of the National Security Information or Restricted Data documents or material (e.g., CONFIDENTIAL National Security Information regarding the physical protection of strategic special nuclear material) to be handled.

6.0 PERSONNEL SECURITY

6.1 Requests for NRC Access Authorization

Describe how requests for access authorization will be handled and controlled to ensure that each individual submitted for NRC access authorization requires access to classified information at the level requested ("Q" or "L") in connection with NRC licensing/certifying activities. This would include all access authorizations requested under the sponsorship of licensee/certificate holder-related activities (e.g., employees, consultants and contractors). Also, identify what the requests for access authorization include (e.g., SF 86, "Questionnaire for National Security Positions," Part 1 and 2, two fingerprint cards, SF 176, "Security Acknowledgment," and other related forms as required). (10 CFR 25.17(a), (b), and (c))

6.2 Review and Control of NRC Access Authorization Processing

Describe the review and control measures to be established to ensure the completeness, accuracy, legibility, and timeliness of information necessary for access authorization processing and the submittal of the appropriate fees. (10 CFR 25.17(e)&(f))

6.3 Confidentiality of Information

Describe the measures to protect the confidentiality of information in SF 86, "Questionnaire for National Security Positions" before its submission to the NRC Division of Facilities and Security. (10 CFR 25.17 (b))

6.4 Cancellation of NRC Access Authorization Requests

Describe the measures to ensure timely notification to the Cognizant Security Agency (CSA) when an individual's request for access authorization is to be withdrawn or canceled. (10 CFR 25.25)

6.5 Handling of Security Terminations

Identify the conditions under which an employee's access authorization is to be terminated.

Describe the procedure for recovering classified data/material from individuals whose access authorization has been terminated.

Describe the methods to obtain NRC Form 136s,"Security Termination Statement" from individuals who hold NRC access authorization under the licensee interest but no longer require NRC access authorization. (10 CFR 25.33)

6.6 Continued Eligibility for NRC Access Authorization

Describe the measures taken to ensure timely notification to the CSA of developments bearing on an individual's continued eligibility for NRC access authorization. (10 CFR 25.21(b))

Describe the procedure for ensuring timely submissions for the renewal of access authorizations. (10 CFR 25.21(c))

6.7 Notification of Grant of Access Authorization

Upon receipt of notification of grant of access authorization, describe the procedure for ensuring timely execution and submission of a SF-312, "Classified Information Nondisclosure Agreement" by the individual and when a security orientation briefing will be provided. (10 CFR 25.23) and (10 CFR 95.33)

6.8 Classified Visits

Describe in detail how requests for Classified Visits will be handled and controlled to ensure that they meet the requirements of 10 CFR 25.35(a) thru (e).

7.0 RECORDS MAINTENANCE

Each licensee, certificate holder, or other persons approved for personnel security access authorization under 10 CFR Part 25, will maintain records as prescribed within 10 CFR Part 25. These records are subject to review and inspection by the Cognizant Security Agency (CSA) representatives during security reviews.
(10 CFR 25.13(a))

Each licensee, certificate holder or other person granted Facility Security Clearance under 10 CFR Part 95 will maintain records prescribed within 10 CFR Part 95. These records are subject to review and inspection by CSA representatives during security reviews. (10 CFR 95.13(a))

Each record required by 10 CFR Parts 25 and 95 must be legible throughout the retention period specified by each Commission regulation. The record may be the original or a reproduced copy or a microform provided that the copy or microform is authenticated by authorized personnel and that the microform is capable of producing a clear copy throughout the required retention period. The record may also be stored in electronic media with the capability for producing legible, accurate, and complete records during the required retention period. Records such as letters, drawings, specifications, must include all pertinent information such as stamps, initials, and signatures. The licensee, certificate holder, or other organization shall maintain adequate safeguards against tampering with and loss of records. (10 CFR 25.13(b))(10 CFR 95.13(b))

Describe the methods used to ensure that the following records are being maintained by the licensee, certificate holder or related organization:

a. Records of access authorization grant and renewal notification must be maintained by the licensee, certificate holder, or other organization for 3 years after the access authorization has been terminated by the CSA. (10 CFR 25.23)

b. Records reflecting an individual's initial and refresher security orientations and security termination must be maintained for 3 years after termination of the individual's access authorization. (10 CFR 95.33(h))

c. Records regarding visits and inspections by representatives of the International Atomic Energy Agency or by participants in other international agreements must be maintained for 5 years beyond the date of the visit or inspection. These

records must specifically identify each document which has been released to an authorized representative and indicate the date of the release. These records must also identify (in such detail as the Division of Facilities and Security, by letter, may require) the categories of documents that the authorized representative has had access and the date of this access. A licensee, certificate holder or other person subject to 10 CFR Part 95 shall also retain Division of Facilities and Security disclosure authorizations for 5 years beyond the date of any visit or inspection when access to classified information was permitted. (10 CFR 95.36(d))

d. Records reflecting accountability and disposition of classified matter must be maintained for 3 years after its disposition. Each licensee, certificate holder, or other person subject to 10 CFR Part 95 possessing matter classified as SECRET National Security Information and/or Restricted Data shall establish an accountability procedure and shall maintain records to show the disposition of such matter. (10 CFR 95.41)

e. Records identifying the sender from which the material was received or recipient to which the material was dispatched. Receipt and dispatch records must be retained for 2 years. (10 CFR 95.41(e))

8.0 PROTECTION OF CLASSIFIED INFORMATION/MATERIAL IN STORAGE

The protection of SECRET matter requires that it be stored in a security container or an approved security area under the protection of a NRC approved intrusion alarm system or protective personnel. CONFIDENTIAL matter in storage must be protected in a manner consistent with SECRET or in a locked security container or approved security area within a locked room or building.

Describe the type of container (manufacture, class, and locking mechanism) or security area which will be used for the storage of SECRET and CONFIDENTIAL matter. (10 CFR 95.25 (a)&(b))

8.1 Intrusion Alarm Systems

Describe in detail the type of intrusion detection system that will be used for the protection of open shelf or bin storage of classified matter in a Closed Area. (10 CFR 95.29(b)(6) and 95.29(c)(4))

8.1.1 Alarm Types

Identify the generic types of intrusion detection sensors used (e.g., electro-mechanical or volumetric). Provide a complete list of the specific

intrusion detection sensors (e.g., balanced magnetic door contacts, infrared) including the manufacturer and model numbers.

8.1.2 Alarm Zones

Each individual intrusion detection sensor or group of sensors which has been configured to provide a unique annunciation at the central alarm station to identify an intrusion into a specific area or location, is identified as an alarm zone. Provide a complete list and description of all alarm zones which protect NRC classified matter.

8.1.3 Central Alarm Station

Identify the location and describe the security provided for the Central Alarm Station (CAS). Describe the staffing of the CAS and any coordination and communications provided between the CAS and protective personnel and local law enforcement authorities.

8.1.4 Alarm Zone Annunciation

Describe the intrusion alarm annunciation system and give the manufacturer's name and model number of the annunciator(s) provided at the CAS. Indicate whether individual alarm zones are visually and/or audibly annunciated. Describe how the system confirms that the system is ready to annunciate an intrusion attempt after being reset for an alarm condition in any given alarm zone or combination of zones. Indicate whether a recording device is utilized to record the time, date, and status of the intrusion alarm system and, if so, give the manufacturer's name and model number of the recording equipment.

8.1.5 Access Mode of Operation

Identify when alarm zones are operated in the access mode. Describe the procedure for accessing and securing alarm zones and how such is annunciated at the CAS.

8.1.6 Line Security

Describe the protection provided the alarm lines between the protected area and the CAS (e.g., electronic line supervision). Also, describe how tampering with the alarm lines will be annunciated at the CAS.

8.1.7 Tamper Protection

Describe the protection provided, if any, to detect attempted tampering with components (e.g., alarm sensors, electrical cabinets) of the intrusion alarm system. Describe how tamper alarms will be annunciated at the CAS.

8.1.8 Emergency Power

Describe the type, source and location of standby, backup, or emergency power provided to maintain continuity of operation of the intrusion alarm system in case of loss of primary facility power. Identify the capacity, in hours, of the emergency power system. Note if there is any loss of alarm capability either during the period of changeover from primary to emergency power or any degradation of the intrusion alarm system operation while on emergency power. Indicate if the intrusion alarm system annunciates the status of the emergency power system and if it annunciates system operation in the emergency power mode.

8.1.9 Local Alarm Annunciation

Identify the location, purpose and type (e.g., bell, siren, lamps) of any local alarm annunciation.

8.2 Protective Personnel

8.2.1 General Description

Describe and discuss the requirements when protective personnel will be used and provide the number of guards or watchmen that will be used for the protection of classified matter.

Describe their functions, security clearance levels and orders. (10 CFR 95.31)

8.2.2 Selection

Describe the method of screening and selecting protective personnel used for the protection of classified matter.

8.2.3 Training

Provide an outline of the security force training program related to the protection of classified matter.

8.2.4 Qualifications

Discuss the methods to be used to assure that each protective personnel member who will be assigned to protect classified matter is qualified to perform the assigned duties. Discuss the means to requalify protective personnel.

8.2.5 Posts

Identify the location and function of each post at which protective personnel will be stationed to safeguard classified matter.

8.2.6 Patrols

Describe protective personnel patrols during both normal working and nonworking hours.

8.2.7 Communications

Specify the types of communications utilized by protective personnel, (e.g. portable/mobile radios with/without DES encryption, cellular phones, and special purpose radios).

8.3 Physical Checks

Protective personnel when used shall conduct patrols during non-working hours at least every 8 hours and more frequently if necessary to maintain a commensurate level of protection for the material in storage as outlined in 10 CFR 95.25 and 95.27. Entrances to Restricted or Closed Areas must be continuously monitored by protective personnel or by an approved alarm system. (10 CFR 95.29(b)(6))

Describe how this function will be fulfilled and monitored.

8.4 Classified Lock Combinations

8.4.1 Records

A minimum number of authorized persons may know the combinations to authorized storage containers. Security containers, vaults, cabinets, and other authorized storage containers must be kept locked when not under the direct supervision of an authorized person entrusted with the contents. Describe how this requirement will be met. (10 CFR 95.25(c)(l))

8.4.2 Conditions Under Which Combinations Must Be Changed

Describe when combinations will be changed by a person authorized access to the contents of the container, or by the FSO or his or her designee. The discussion should include:

a. The initial use of an approved container or lock for the protection of classified material;

b. The termination of employment of any person having knowledge of the combination, or when the clearance granted to any such person has been withdrawn, suspended, or revoked;

c. The compromise or suspected compromise of a container or its combination, or discovery of a container left unlocked and unattended; or

d. At other times when considered necessary by the FSO or CSA.

Describe the system to be used to ensure these requirements are met. (10 CFR 95.25(c)(2))

8.4.3 Records of Combination

Records of combinations shall be classified, marked, and safeguarded in a manner appropriate for the highest classification and category of the matter authorized to be stored in the security container. Describe how this requirement will be accomplished. (10 CFR 95.25(d))

8.4.4 Selection of Combinations

Each combination must be randomly selected and require the use of at least three different numbers. In selecting combinations, multiples, simple arithmetical ascending or descending series, telephone numbers, social security numbers, car license numbers and calendar dates such as birth dates and anniversaries, shall be avoided. Describe the method to be used to ensure this requirement will be met. (10 CFR 95.25(e))

8.4.5 Cautions Regarding Combinations and Authority to Change Combinations

Combinations shall be changed only by persons authorized access to SECRET or CONFIDENTIAL National Security Information and/or Restricted Data, depending upon the matter authorized to be stored in, the security container. Describe how combinations will be changed. (10 CFR 95.25(f))

8.5 Posted Information

Containers may not bear external markings indicating the level of classified material authorized for storage. A record of the names of persons having knowledge of the combination must be posted inside the container. Indicate how this will be accomplished. (10 CFR 95.25(g))

8.6 End of Day Security Checks

Facilities that store classified material shall establish a system of security checks at the close of each working day or at the last working shift of each day to ensure that all classified material and security repositories have been appropriately secured. Describe what measures will be used to ensure this requirement will be met.
(10 CFR 95.25(h)(1)&(2))

8.7 Unattended Security Container Found Open

If an unattended security container housing classified matter is found unlocked, the custodian or an alternate must be notified immediately. The container must be secured by protective personnel or a properly cleared employee and an effort must be made to determine if the contents were compromised not later than the next day. (10 CFR 95.25(i))

8.8 Key Control

Describe the procedures whereby the supervision of keys to locks for Security Areas will meet the requirements of 10 CFR 95.25(j).

9.0 PROTECTION OF CLASSIFIED MATTER WHILE IN USE

While in use, classified matter must be under the direct control of an authorized individual to preclude physical, audio, and visual access by persons who do not have the prescribed access authorization or other written CSA disclosure authorization (see 10 CFR 95.36 for additional information concerning disclosure authorizations). Describe how this requirement will be accomplished. (10 CFR 95.27)

10.0 ESTABLISHMENT OF RESTRICTED OR CLOSED AREAS

If, because of its nature, sensitivity or importance, matter containing classified information cannot otherwise be effectively controlled in accordance with the provisions of 10 CFR 95.25 and 95.27, a Restricted or Closed area must be established to protect such matter. (10 CFR 95.29 (a))

a. Describe in detail why and how a Restricted Area will be used which meets the following security requirements: (10 CFR 95.29(b))

1. Restricted areas must be separated from adjacent areas by a physical barrier designed to prevent unauthorized access (physical, audio, and visual) into these areas.

2. Controls must be established to prevent unauthorized access to and removal of classified matter.

3. Access to classified matter must be limited to persons who possess appropriate access authorization or other written CSA disclosure authorization and who require access in the performance of their official duties or regulatory obligations.

4. Persons without appropriate access authorization for the area visited must be escorted by an appropriate CSA access authorized person at all times while within Restricted or Closed areas.

5. Each individual authorized to enter a Restricted or Closed area must be issued a distinctive form of identification (e.g., badge) when the number of employees assigned to the area exceeds thirty per shift.

6. During non-working hours, admittance must be controlled by personnel. Protective personnel shall conduct patrols during non-working hours at least every 8 hours and more frequently if necessary to maintain a commensurate level of protection. Entrances must be continuously monitored by protective personnel or by an approved alarm system.

b. Due to the size and nature of the classified material, or operational necessity, it may be necessary to construct Closed Areas for storage because GSA-approved containers or vaults are unsuitable or impractical. Closed Areas must be approved by the CSA. Describe in detail why and how a closed area will be used which meets the following security requirements: 10 CFR 95.29(c))

1. Access to Closed Areas must be controlled to preclude unauthorized access. This may be accomplished through the use of a cleared employee or by a CSA approved access control device or system.

2. Access must be limited to authorized persons who have an appropriate security clearance and a need-to-know for the classified material/information within the area. Persons without the appropriate level of clearance and/or need-to-know must be escorted at all times by

an authorized person where inadvertent or unauthorized exposure to classified information cannot otherwise be effectively prevented.

3. The Closed Area must be accorded supplemental protection during non-working hours. During these hours, admittance to the area must be controlled by locked entrances and exits secured by either an approved built-in combination lock or an approved combination or key-operated padlock. However, doors secured from the inside with a panic bolt (for example, actuated by a panic bar), a dead bolt, a rigid wood or metal bar, or other means approved by the CSA, do not require additional locking devices.

4. Open shelf or bin storage of classified documents in Closed Areas requires CSA approval. Only areas protected by an approved intrusion detection system will qualify for approval.

11.0 SECURITY EDUCATION

Describe how the requirements of 10 CFR 95.33 will be met so that all cleared employees are provided with security training and briefings commensurate with their involvement with classified information. The facility may obtain defensive security, threat awareness, and other education and training information and material from their CSA or other sources. Your description should include:

a. FSO Training. Licensees, certificate holders and others are responsible for ensuring that the FSO, and others performing security duties, complete security training deemed appropriate by the CSA. Training requirements must be based on the facility's involvement with classified information and may include a FSO orientation course and, for FSOs at facilities with safeguarding capability, a FSO Program Management Course. Training, if required, should be completed within 1 year of appointment to the position of FSO. Describe in detail how this requirement will be met.

b. Temporary Help Suppliers. A temporary help supplier, or other contractor who employs cleared individuals solely for dispatch elsewhere, is responsible for ensuring that required briefings are provided to their cleared personnel. The temporary help supplier or the using licensee, certificate holder, or other facility may conduct these briefings. Describe in detail how this requirement will be met.

c. Classified Information Non-disclosure Agreement (SF-312). The SF-312 is an agreement between the United States and an individual who is cleared for access to classified information. An employee issued an initial personnel security clearance must, in accordance with the requirements of 10 CFR 25.23, execute

an SF-312 before being granted access to classified information. The FSO shall forward the executed SF-312 to the CSA for retention. If the employee refuses to execute the SF-312, the licensee, certificate holder, or other facility shall deny the employee access to classified information and submit a report to the CSA. The SF-312 must be signed and dated by the employee and witnessed. The employee's and witness' signatures must bear the same date. Describe in detail how this requirement will be met.

d. Initial Security Briefings. Before being granted access to classified information, an employee shall receive an initial security briefing that includes the following topics:

1. A Threat Awareness Briefing.

2. A Defensive Security Briefing.

3. An overview of the security classification system.

4. Employee reporting obligations and requirements.

5. Security procedures and duties applicable to the employee's job.

Describe in detail how you will meet these requirements.

e. Refresher Briefings. The licensee, certificate holder, or other facility shall conduct periodic refresher briefings for all cleared employees every 3 years. As a minimum, the refresher briefing must reinforce the information provided during the initial briefing and inform employees of appropriate changes in security regulations. This requirement may be satisfied by use of audio/video materials and by issuing written materials on a regular basis. Describe in detail how this requirement will be met.

f. Debriefings. Licensees, certificate holders, and others shall debrief cleared employees at the time of termination of employment (discharge, resignation, or retirement); when an employee's access authorization is terminated, suspended, or revoked; and upon termination of the Facility Security Clearance. Describe in detail how this requirement will be met.

g. Derivative Classifier and Declassifier Training. Licensees, certificate holders, and other facilities must establish and maintain a security education and training program for derivative classifiers, declassification authorities, security managers, classification management officers, security specialists,

and all other personnel whose duties significantly involve the creation or handling of classified information. Describe in detail how this requirement will be met. (32 CFR 2001.41)

12.0 ACCESS TO MATTER CLASSIFIED AS NATIONAL SECURITY INFORMATION AND RESTRICTED DATA

Describe how access to classified matter will be controlled in accordance with the following procedures and requirements in 10 CFR 95.35:

a. Except as the NRC Commission may authorize, no person subject to the regulations in 10 CFR Part 95 may receive or may permit any individual to have access to matter revealing SECRET or CONFIDENTIAL National Security Information or Restricted Data unless the individual has:

1. A "Q" access authorization which permits access to matter classified as SECRET and CONFIDENTIAL Restricted Data or SECRET and CONFIDENTIAL National Security Information which includes intelligence information, CRYPTO (i.e., cryptographic information) or other classified communications security (COMSEC) information, or

2. An "L" access authorization which permits access to matter classified as CONFIDENTIAL Restricted Data and SECRET and CONFIDENTIAL National Security Information other than that noted in paragraph (a)(1) of this section except that access to certain CONFIDENTIAL COMSEC information is permitted as authorized by a National Communications Security Committee waiver dated February 14, 1985.

3. An established "need-to-know" for the matter (See Definitions, 10 CFR 95.5).

4. NRC-approved storage facilities if classified documents or material are to be transmitted to the individual.

b. Matter classified as National Security Information or Restricted Data shall not be released by a licensee, certificate holder, or other person subject to 10 CFR Part 95 to any personnel other than properly access authorized Commission licensee employees, or other individuals authorized access by the Commission.

c. Access to matter which is National Security Information at NRC-licensed facilities or NRC-certified facilities by authorized representatives of IAEA is permitted in accordance with 10 CFR 95.36.

12.1 Access by representatives of the International Atomic Energy Agency or by participants in other international agreements.

Describe the controls, procedures and record keeping processes used to meet and comply with the following requirements in 10 CFR 95.36:

a. Based upon written disclosure authorization from the NRC Division of Facilities and Security that an individual is an authorized representative of the International Atomic Energy Agency (IAEA) or other international organization and that the individual is authorized to make visits or inspections in accordance with an established agreement with the United States Government, a licensee, certificate holder or other person subject to this part shall permit the individual (upon presentation of the credentials specified in 10 CFR 75.7 and any other credentials identified in the disclosure authorization) to have access to matter classified as National Security Information that is relevant to the conduct of a visit or inspection. A disclosure authorization under 10 CFR 95.36 does not authorize a licensee, certificate holder, or other person subject to this part to provide access to Restricted Data.

b. For purposes of 10 CFR 95.36, Classified National Security Information is relevant to the conduct of a visit or inspection if–

   1. In the case of a visit, this information is needed to verify information according to 10 CFR 75.13; or

   2. In the case of an inspection, an inspector is entitled to have access to the information under 10 CFR 75.42.

c. In accordance with the specific disclosure authorization provided by the NRC Division of Facilities and Security, licensees, certificate holders, or other persons subject to this part are authorized to release (i.e., transfer possession of) copies of documents which contain Classified National Security Information directly to IAEA inspectors and other representatives officially designated to request and receive Classified National Security Information documents. These documents must be marked specifically for release to IAEA or other international organizations in accordance with instructions contained in the NRC's disclosure authorization letter. Licensees, certificate holders, or other persons subject to this part may also forward these documents through the NRC to the international organization's headquarters in accordance with the NRC disclosure authorization. Licensees, certificate holders, and other persons may not reproduce documents containing Classified National Security Information except as provided in 10 CFR 95.43.

d. Records regarding these visits and inspections must be maintained for 5 years beyond the date of the visit or inspection. These records must specifically identify each document which has been released to an authorized representative and indicate the date of the release. These records must also identify (in such detail as the NRC Division of Facilities and Security, by letter, may require) the categories of documents that the authorized representative has had access and the date of this access. A licensee, certificate holder, or other person subject to this part shall also retain NRC Division of Facilities and Security disclosure authorizations for 5 years beyond the date of any visit or inspection when access to classified information was permitted.

e. Licensees, certificate holders, or other persons subject to this part shall take such measures as may be necessary to preclude access to classified matter by participants of other international agreements unless specifically provided for under the terms of a specific agreement.

13.0 CLASSIFICATION AND PREPARATION OF DOCUMENTS

Classified information generated or possessed by a licensee, certificate holder, or other person must be appropriately marked. Classified material which is not conducive to markings (e.g., equipment) may be exempt from this requirement. These exemptions are subject to the approval of the CSA on a case-by-case basis. If a person or facility generates or possesses information that is believed to be classified based on guidance provided by the NRC or by derivation from classified documents, but which no authorized classifier has determined to be classified, the information must be protected and marked with the appropriate classification markings pending review and signature of an NRC authorized classifier. This information shall be protected as classified information pending final determination.

The Facility Security Clearance request must address the following marking requirements: (10 CFR 95.37)

a. Classification consistent with content. Describe the process that will ensure that each document containing classified information shall be classified SECRET or CONFIDENTIAL according to its content. NRC licensees, certificate holders, or others subject to the requirements of 10 CFR Part 95 may not make original classification decisions.

b. Markings required on face of documents.

1. For derivative classification of Classified National Security Information:

i. Describe the process that will ensure that derivative classifications of Classified National Security Information

contain the identity of the source document or the classification guide, including the agency and office of origin, on the "Derived From" line and its classification date. If more than one source is cited, the "Derived From" line should indicate "Multiple Sources." The derivative classifier shall maintain the identification of each source with the file or record copy of the derivatively classified document.

ii. Declassification instructions. Describe the process that will ensure that when marking derivatively classified documents, the "DECLASSIFY ON" line carries forward the declassification instructions as reflected on the source document. If multiple sources are used, the instructions will carry forward the longest duration.

Derived From_____
(source)
Reason_____
Declassify On: Source Marked "OADR"
Date of Source:_____
Classifier:_____
(Name/Title/Number)

iii. Describe the process that will ensure that if the source document used for derivative classification contains the declassification instruction, "Originating Agency's Determination Required" (OADR), the new document will reflect the date of the original classification of the information as contained in the source document or classification guide. An example of the stamp might be as follows:

Derived From_____
(source)
Reason_____
Declassify On: Source Marked "OADR"
Date of Source:_____
Classifier:_____
(Name/Title/Number)

iv. Describe the process that will ensure that the derivative classifier will maintain the identification of each source with the file or record copy of the derivatively classified document.

2. For Restricted Data documents:

i. Describe the process that will ensure the identity of the classifier. The identity of the classifier must be shown by completion of the "Derivative Classifier'' line. The "Derivative Classifier" line must show the name of the person classifying the document and the basis for the classification. Dates for downgrading or declassification do not apply.

ii. Describe the process that will ensure classification designation (e.g., SECRET, CONFIDENTIAL) and Restricted Data are placed on all classified documents. NOTE: No "Declassification" instructions will be placed on documents containing Restricted Data.

c. Placement of markings. Describe the process that will ensure that the highest classification marking assigned to a document will be placed in a conspicuous fashion in letters at the top and bottom of the outside of the front covers and title pages, if any, and first and last pages on which text appears, on both bound and unbound documents, and on the outside of back covers of bound documents. The balance of the pages must be marked at the top and bottom with:

1. The overall classification marking assigned to the document;

2. The highest classification marking required by content of the page; or

3. The marking UNCLASSIFIED if they have no classified content.

d. Additional markings.

1. Describe the process that will ensure that if the document contains any form of Restricted Data, it will bear the appropriate marking on the first page of text, on the front cover and title page, if any. For example: "This document contains Restricted Data as defined in the Atomic Energy Act of 1954. Unauthorized disclosure subject to Administrative and Criminal Sanctions."

2. Describe the process that will ensure that limitations on reproductions or dissemination are noted on the document. If the originator or classifier determines that reproduction or further dissemination of a document should be restricted, the following additional wording may be placed on the face of the document:

Reproduction or Further Dissemination Requires Approval of

_____

If any portion of this additional marking does not apply, it should be crossed out.

e. Portion markings. Describe the process that will ensure that in addition to the information required on the face of the document, that each classified document by marking or other means, indicates clearly which portions are classified (e.g., paragraphs or pages) and which portions are not classified. The symbols (S) for SECRET, (C) for CONFIDENTIAL, (U) for Unclassified, or (RD) for Restricted Data may be used immediately preceding or following the text to which it applies, except that the designation must follow titles or subjects. (Portion marking of paragraphs is not required for documents containing Restricted Data). If this type of portion marking is not practicable, the document must contain a description sufficient to identify the classified information and the unclassified information.

Example

Pages 1-3 SECRET
Pages 4-19 Unclassified
Pages 20-26 SECRET
Pages 27-32 CONFIDENTIAL

f. Transmittal document. Describe the process that will ensure that if a document transmitting classified information contains no classified information or the classification level of the transmittal document is not as high as the highest classification level of its enclosures, that the document must be marked at the top and bottom with a classification at least as high as its highest classified enclosure. The classification may be higher if the enclosures, when combined, warrant a higher classification than any individual enclosure. When the contents of the transmittal document warrants a lower classification than the highest classified enclosure(s) or combination of enclosures or requires no classification, a stamp or marking such as the following must also be used on the transmittal document:

UPON REMOVAL OF ATTACHMENTS THIS DOCUMENT IS:
(Classification level of transmittal document standing alone or the word "UNCLASSIFIED" if the transmittal document contains no classified information.)

g. Classification challenges. Describe the process that will ensure that persons in authorized possession of classified National Security Information who in good

faith believe that the information's classification status (i.e., that the document), is classified at either too high a level for its content (over classification) or too low for its content (under classification) are expected to challenge its classification status. Persons who wish to challenge a classification status shall-

1. Refer the document or information to the originator or to an authorized NRC classifier for review. The authorized classifier shall review the document and render a written classification decision to the holder of the information.

2. In the event of a question regarding classification review, the holder of the information or the authorized classifier shall consult the NRC Division of Facilities and Security, Information Security Branch, for assistance.

3. Persons who challenge classification decisions have the right to appeal the classification decision to the Interagency Security Classification Appeals Panel.

4. Persons seeking to challenge the classification of information will not be the subject of retribution.

h. Files, folders or group of documents. Describe the process that will ensure how files, folders, binders, or groups of physically connected documents will be marked at least as high as the highest classified document which they contain.

i. Drafts and working papers. Describe the process that will ensure that drafts of documents and working papers which contain, or which are believed to contain, classified information will be marked as classified information.

j. Classification guidance. Describe the process that will ensure that licensees, certificate holders, or other persons subject to this part will classify and mark classified matter as National Security Information or Restricted Data, as appropriate, in accordance with classification guidance provided by the NRC as part of the Facility Security Clearance process.

k. Changes in Classification. Describe the process that will ensure that documents containing Classified National Security Information must be downgraded or declassified as authorized by the NRC classification guides or as determined by the NRC. Requests for downgrading or declassifying any NRC classified information should be forwarded to the NRC Division of Facilities and Security, Office of Administration, Washington, DC 20555-0001. Requests for downgrading or declassifying of Restricted Data will be forwarded to the NRC

Division of Facilities and Security for coordination with the Department of Energy. State how such actions will be implemented. (10 CFR 95.45(a))

Indicate that if a change of classification or declassification is approved, the previous classification marking must be canceled and the following statement, properly completed, must be placed on the first page of the document: (10 CFR 95.45(b))

Classification canceled (or changed to)

_____

(Insert appropriate classification)
by authority of

_____

(Person authorizing change in classification)

_____

(Signature of person making change and date thereof)

Indicate that new markings reflecting the current classification status of the document will be applied in accordance with the requirements of 10 CFR 95.37. (10 CFR 95.45(c))

Indicate that any persons making a change in classification or receiving notice of such a change shall forward notice of the change in classification to holders of all copies as shown on their records. (10 CFR 95.45(d))

14.0 EXTERNAL TRANSMISSION OF DOCUMENTS AND MATERIAL

Indicate what controls/procedures will be instituted to comply with the following requirements of 10 CFR 95.39 to ensure proper transmission of documents and materials:

a. Restrictions. Documents and material containing classified information received or originated in connection with an NRC license or certificate must be transmitted only to CSA approved security facilities.

b. Preparation of documents. Documents containing classified information must be prepared in accordance with the following when transmitted outside an individual installation.

1. The documents must be enclosed in two sealed opaque envelopes or wrappers.

2. The inner envelope or wrapper must contain the addressee's classified mail address and the name of the intended recipient. The appropriate

classification must be placed on both sides of the envelope (top and bottom) and the additional markings, as appropriate, referred to in 10 CFR 95.37(e) must be placed on the side bearing the address.

3. The outer envelope or wrapper must contain the addressee's classified mail address. The outer envelope or wrapper may not contain any classification, additional marking or other notation that indicates that the enclosed document contains classified information. The Classified Mailing Address shall be uniquely designed for the receipt of classified information. The classified shipping address for the receipt of material(e.g. equipment) should be different from the classified mailing address for receipt of classified documents.

4. A receipt that contains an unclassified description of the document, the document number, if any, date of the document, classification, the date of transfer, the recipient and the person transferring the document must be enclosed within the inner envelope containing the document and be signed by the recipient and returned to the sender whenever the custody of a SECRET document is transferred. This receipt process is at the option of the sender for CONFIDENTIAL information.

c. Methods of transportation.

1. SECRET matter may be transported only by one of the following methods within and directly between the U.S., Puerto Rico, or a U.S. possession or trust territory:

i. U.S. Postal Service Registered Mail.

ii. A cleared "Commercial Carrier."

iii. A cleared commercial messenger service engaged in the intracity/local area delivery (same day delivery only) of classified material.

iv. A commercial delivery company, approved by the CSA, that provides nationwide, overnight service with computer tracing and reporting features. These companies need not be security cleared.

v. Other methods as directed, in writing, by the CSA.

2. CONFIDENTIAL matter may be transported by one of the methods set forth in paragraph (c)(1) of this section, or U.S. Certified Mail. U.S.

Certified mail may be used in transmission of Confidential documents to Puerto Rico or any United States territory of possession.

d. Telecommunication of classified information. Classified information may not be telecommunicated unless the telecommunication system has been approved by the CSA. Licensees, certificate holders or other persons who may require a secure telecommunication system shall submit a telecommunication plan as part of their request for Facility Security Clearance, as outlined in 10 CFR 95.15, or as an amendment to their existing Standard Practice Procedures Plan for the protection of classified information. See section 18.0 below for details regarding secure telecommunications.

e. Security of classified information in transit. Classified matter that, because of its nature, cannot be transported in accordance with 10 CFR 95.39(c), may only be transported in accordance with procedures approved by the CSA. Procedures for transporting classified matter are based on a satisfactory transportation plan submitted as part of the licensee's, certificate holder's, or other person's request for Facility Security Clearance or submitted as an amendment to its existing Standard Practice Procedures Plan.

Indicate what controls/procedures will be instituted to comply with these requirements. (10 CFR 95.39)

14.1 External receipt and dispatch records

Describe how procedures will be implemented to meet the following record keeping requirements of 10 CFR 95.41:

a. The date of the material;

b. The date of receipt or dispatch;

c. The classification;

d. An unclassified description of the material; and

e. The identity of the sender from which the material was received or recipient to which the material was dispatched.

Receipt and dispatch records must be retained for 2 years.

15.0 AUTHORITY TO REPRODUCE CLASSIFIED INFORMATION

Describe the controls and procedures to meet the following requirements from 10 CFR 95.43:

Each licensee, certificate holder, or other person possessing classified information shall establish a reproduction control system to ensure that reproduction of classified material is held to the minimum consistent with operational requirements. Classified reproduction must be accomplished by authorized employees knowledgeable of the procedures for classified reproduction. The use of technology that prevents, discourages, or detects the unauthorized reproduction of classified documents is encouraged. Identify the types of machines and the controls on machines used for reproduction.

Unless restricted by the CSA, SECRET and CONFIDENTIAL documents may be reproduced. Reproduced copies of classified documents are subject to the same protection as the original documents.

All reproductions of classified material must be conspicuously marked with the same classification markings as the material being reproduced. Copies of classified material must be reviewed after the reproduction process to ensure that these markings are visible.

Also, identify the types of machines and the controls on machines used for reproduction and discuss the disposition of extra and defective copies.

16.0 DESTRUCTION OF MATTER CONTAINING NATIONAL SECURITY INFORMATION AND RESTRICTED DATA

Documents containing classified information may be destroyed by burning, pulping, or another method that ensures complete destruction of the information that they contain. The method of destruction must preclude recognition or reconstruction of the classified information. Any doubts on methods should be referred to the CSA.

Indicate what controls/procedures will be instituted to comply with these requirements. (10 CFR 95.47)

17.0 REPORTS TO THE NRC

Each licensee, certificate holder, or other person having a Facility Security Clearance shall immediately report to the CSA and the Regional Administrator of the appropriate NRC Regional Office listed in appendix A, 10 CFR Part 73:

a. Any alleged or suspected violation of the Atomic Energy Act, Espionage Act, or other Federal statutes related to classified information. (e.g., deliberate disclosure of classified information to persons not authorized to receive it, theft of classified information). Incidents such as this must be reported within 1 hour of the event followed by written confirmation within 30 days of the incident.

b. Any infractions, losses, compromises or possible compromise of classified information or classified documents not falling within paragraph (a) of this section. Incidents such as these must be entered into a written log. A copy of the log must be provided to the NRC on a monthly basis. Details of security infractions including corrective action taken must be available to the CSA upon request.

c. In addition, NRC requires records for all classification actions (documents classified, declassified, or downgraded) to be submitted to the NRC Division of Facilities and Security. These may be submitted either on an "as completed" basis or monthly. The information may be submitted either electronically by an on-line system (NRC prefers the use of a dial-in automated system connected to the Division of Facilities and Security) or by paper copy using NRC Form 790.

Indicate what controls/procedures will be instituted to comply with these requirements. (10 CFR 95.57)

18.0 SECURE TELECOMMUNICATIONS

Telecommunications systems prepare, transmit, communicate, or process information (e.g., writing, images, sounds) by electrical, electromagnetic, electro mechanical, electro-optical or electronic means, using media such as telephone lines, cable, microwave, satellite, etc. Telecommunications systems include, but are not limited to, telephones, facsimiles, radios, video and video-teleconferencing, networks (LANs, WANs, etc.), or other data transmission systems.

Classified information may not be telecommunicated unless the telecommunications system has been approved by the CSA. Licensees, certificate holders, or other persons who may require secure telecommunications capability shall submit a secure telecommunications plan as part of their request for Facility Security Clearance, as outlined in 10 CFR 95.15, or as an amendment to their existing Standard Practice Procedures Plan for the protection of classified information. The plan submitted for NRC approval should include the following:

18.1 Justification for the Need for Secure Telecommunications

Justify the need for secure voice and/or data communications. Discuss the classification levels (e.g., SECRET or CONFIDENTIAL); categories of information (e.g., NSI or RD); and the types of information (e.g., material control and accountability information) being transmitted.

18.2 Duration and Nature of Activity

Indicate if this is an on-going requirement, or if short-term, the probable duration of the telecommunications activity.

18.3 Supplementary Glossary of Terms

Define any special terminology applicable to the telecommunications system which may be system unique or is not defined in National Security Telecommunications and Information Systems Security Instruction NSTISSI No. 4009, "National Information Systems Security (INFOSEC) Glossary."

The terms "Secure Communications Center" and "Telecommunications Facility," refer to a type of facility dedicated to the preparation, transmission, communication or related processing of information. Unless otherwise noted, both terms refer to both attended and unattended facilities.

18.4 Equipment and Media

List all equipment and media that comprises the secure telecommunications system, including terminal equipment, cryptographic equipment, modems, switching systems, signaling equipment, testing equipment. If the telecommunications system is networked, describe the network media used, e.g., twisted pair cable, coaxial cable, fiber optic cable, microwave, satellite, or combinations of media (i.e., a network system that uses Ethernet cabling throughout a building, but fiber optic cabling between buildings).

Provide the manufacturer's name and the model number of each piece of equipment.

18.5 System Functional Block Diagram

By means of a complete system functional block diagram, show the functional interrelationship of all equipment associated with the secure telecommunications system, including terminal equipment, cryptographic equipment, and modems. If the telecommunications system is networked, provide the network security architecture, specifically addressing security-relevant issues. All interconnected nodes on the

network should be provided on the block diagram. Provide a brief narrative description as necessary to supplement the diagram.

18.6 COMSEC

COMSEC is a program in which the National Security Agency (NSA) acts as the central procurement agency for the development and, in some cases, the production of INFOSEC items. The NSA certifies cryptographic and other communications security products such as key, equipment, devices, documents, firmware, or software that embodies or describes cryptographic logic or performs COMSEC functions. COMSEC is considered especially sensitive because of the need to safeguard U.S. cryptographic principles, methods, and material against exploitation.

18.6.1 COMSEC Accounts

COMSEC accounts are administrative entities, identified by an account number, used to maintain accountability, custody, and control of COMSEC material. Discuss the COMSEC account(s) which exists or is planned. Provide the name, address, and telephone number of the Central Office of Record (COR) of the COMSEC account (if already established).

Discuss the contents of the COMSEC account inventory in general terms only (i.e., the holdings in this account include STU-III telephones, Type 1 seed key, traditional key, electronic key, KG-84's, DES key). If additional information is required, the NRC will contact the COR of the account.

NOTE: The information provided in this section may be different from equipment listed in 18.4. Not all equipment and material associated with a telecommunications system is COMSEC accountable.

18.6.2 COMSEC Custodians and Alternates

Designate the names, titles, and qualifications (citizenship, possess a valid "Q" clearance, COMSEC or related experience, training) of the individuals who have been selected as the COMSEC Custodian and Alternate(s).

Because of the sensitivity of COMSEC material and the rigid controls required, the COMSEC Custodian and Alternate(s) must possess exemplary qualities. Ensure that the individuals selected:

a. Are responsible individuals qualified to assume the duties and responsibilities of a COMSEC Custodian;

b. Are in a position or level of authority which will permit them to exercise proper jurisdiction in fulfilling their responsibilities;

c. Have not been previously relieved of COMSEC Custodian duties for reasons of negligence or non-performance of duties;

d. Are in a position which will permit maximum tenure (not less than one year);

e. Will not be assigned duties which will interfere with their duties as COMSEC Custodian or Alternate;

f. Are actually performing the custodial functions on a day-to-day basis. The COMSEC Custodian position will not be assumed solely for the purpose of maintaining administrative or management control of the account functions; and

g. Hold a minimum of a federal government grade of GG-7 or civilian equivalent.

18.6.3 COMSEC Material Accountability

Describe how the accountability of COMSEC materials and documents is maintained (e.g., under NRC oversight, DOE oversight, or NSA oversight, etc.).

18.6.4 Storage, Transportation, Reproduction, and Destruction of COMSEC Material

NSTISSI No. 4005, "Safeguarding COMSEC Facilities and Material," establishes the minimum national standards for safeguarding COMSEC material. Describe how COMSEC material is/will be stored, transported, reproduced, protected, and destroyed. In the case of destruction of accountable COMSEC documents and keying material, state the type, manufacturer, and model number of any destruction equipment (e.g., shredders) you would like to have considered by the CSA as approved equipment. Describe the techniques used in the destruction process (e.g., mixture of classified material with unclassified material, and the method of disposal of the waste material).

18.6.5 COMSEC Training

Discuss COMSEC training (e.g., ND-112, NSA COMSEC Custodian Course) previously received (include dates) by COMSEC Custodian or Alternates (e.g., DOE COMSEC training, NSA COMSEC training, etc.). Indicate the number of people requiring training, the approximate timing for such training, and the name and title of the individual who will coordinate the training.

18.7 Fixed COMSEC Facilities, Telecommunications Facilities, Secure Communications Centers

NSTISSI No. 4005, "Safeguarding COMSEC Facilities and Material," establishes the minimum national standards for constructing and protecting Communications Security (COMSEC) facilities wherein the primary purpose is generating, storing, repairing, or using COMSEC material.

Work areas not considered COMSEC facilities which contain COMSEC equipment (e.g., STU-IIIs, KG-84s, Data Transfer Devices) must be protected in a manner that affords protection at least equal to what is normally provided to other high value/sensitive material, and ensures that access and accounting integrity is maintained.

18.7.1 Physical Security

Describe the physical location of the facility within its host building. Discuss the functions and relative locations of adjacent buildings and rooms. Describe the construction of the facility, to include walls, floors, ceilings, main entrance door, other doors, door locks, windows, other openings, and security systems in place (e.g., intrusion alarms, armed guards, video cameras, etc.).

Describe the procedures for daily security checks (e.g., visual checks are made at least once every 24 hours on a random basis by personnel assigned to the facility).

Provide initial and latest reinspection reports, Technical Security Evaluation (TSE) report, and TEMPEST Countermeasures and Verification reports (if applicable).

18.7.2 Access Lists

Discuss requirements for access to the secure facility. Include the functional titles of the individuals who will routinely access the facility. Provide the title of the official who will generate the access lists and the method to be used for keeping the list up-to-date.

18.7.3 Visitor Control

A visitor register must be maintained at the facility entrance area to record the arrival and departure of authorized visitors. Describe the format of the log, requirements for the monitoring of visitors while in the facility, how personnel security clearances are verified, and what personal identification is required for access to the facility.

18.7.4 Intrusion Alarm System/Protective Personnel

Describe the type of intrusion alarm system (e.g., infrared, ultrasonic) used to protect the facility and where the alarm annunciates. Specify the required response time of protective personnel, if the alarm is activated.

18.7.5 Protecting Passwords and Lock Combinations

Describe the method used for protecting combinations for the secure facility. Refer to NSTISSI No. 4005, "Safeguarding COMSEC Facilities and Material," for the requirements for controlling the combinations of containers used to store COMSEC documents and material. Describe the written instructions furnished to the secure facility's personnel and users for controlling combinations.

18.7.6 Destruction

Identify the pertinent types of classified media (e.g., printed or magnetic storage media) involved in the activities of the secure facility and the classification of the media (e.g., SECRET-National Security Information, SECRET-Restricted Data).

Describe the methods of both routine and emergency destruction of each type of media (e.g., shredding, degaussing). See NSTISSI No. 4004, "Routine Destruction and Emergency Protection of COMSEC Material (U)," for guidance in the destruction of COMSEC Material.

18.7.7 Floor Plans and Drawings

Provide the following:

a. Floor plans of the secure facility showing the location of all equipment, including all terminals, related cryptographic equipment, modems, and other telecommunications equipment.

b. Floor plans showing the construction of walls, floor, and ceiling of the room(s) containing the secure equipment.

c. Separate architectural details such as doors, windows and ducts.

d. Floor plans which indicate the type of facilities and operations in the areas adjacent to and on the floors immediately above and below the secure facility.

e. Installation drawings, including wiring diagrams and conduit plans for the secure telecommunications equipment.

18.7.8 TEMPEST

TEMPEST is an unclassified short name referring to investigations and studies of compromising emanations. Compromising emanations are unintentional intelligence bearing signals that, if intercepted and analyzed, will disclose classified information when it is transmitted, received, handled, or otherwise processed by any information processing equipment.

TEMPEST countermeasures will be applied only in proportion to the threat of exploitation and the resulting damage to the national security, should the information be obtained by a foreign intelligence organization.

If TEMPEST countermeasures are in use at the facility, describe your implementation of the program (e.g., certification, accreditation, zoning, shielding). If TEMPEST is not currently in place, TEMPEST countermeasures, if necessary, will be provided by the CSA on a case-by-case basis.

18.7.9 Nonessential Audio Visual Equipment

Certain U.S. Government owned or leased (or company owned or leased) items are prohibited in secure facilities unless approved by the CSA for conduct of official duties. These include two-way transmitting equipment, recording equipment (audio, video, optical), test measurement, and diagnostic equipment. Also, certain personally owned electronic equipment items, such as photographic, video, and audio recording equipment; and computers and associated media, are prohibited in secure facilities.

Describe in the plan any telephone, intercom, paging, or music systems that are internal to, or penetrate the secure facility. Verify and certify that there are no fortuitous conductors, speakers that can be reversed to be used as

microphones, or telephones that can be rewired to be used as microphones. Pay particular attention to any wire penetrations into the secure facility by any system operated or controlled from outside the facility. This section of the plan should also describe the controls and restrictions imposed on personnel bringing electronic devices into the secure facility.

18.7.10 Technical Security Evaluation (TSE)

All reasonable countermeasures should be taken to ensure that there are no clandestine surveillance devices in secure telecommunications facilities. Evaluations for clandestine surveillance devices should be conducted as appropriate to the threat level determined by the CSA. Such evaluations should be considered when facilities are initially activated or reactivated after foreign occupation, or when there is known or suspected access by foreign maintenance or construction personnel, or when clandestine surveillance or recording devices are suspected in or near a secure facility. Any actual or suspected clandestine surveillance or recording devices must be reported in accordance with the requirements of NSTISSI No. 4003, "Reporting and Evaluating COMSEC Incidents."

Describe any tests or inspections of the secure facility that are planned or have already been performed. Indicate the frequency of the testing; the reason for the frequency (e.g., type, purpose, and classification level of the information handled at the secure facility; or specific equipment contained therein); and, if the tests and inspections include external sound attenuation tests and audio countermeasure tests to detect clandestine "eavesdropping" devices.

Provide a list of tests to be performed, copies of the specific test procedures to be used, and the name of the contractor(s) performing the tests to the NRC Director, Division of Facilities and Security, for approval. If the tests have already been conducted, provide a copy of the test results to the NRC Director, Division of Facilities and Security, for approval.

18.7.11 COMSEC Inspections

A COMSEC inspection should be conducted prior to initial activation where practical, but must be conducted within 90 days after activation. Thereafter, facilities must be reinspected based on threat, physical modifications, sensitivity of programs, and past security performance. At a minimum, the inspection must address secure operating procedures and practices, handling and storage of COMSEC material, and routine and emergency destruction capabilities.

Describe the procedures, either in place or planned, for conducting COMSEC inspections.

18.7.12 Unattended Secure Telecommunications Facilities

Unattended secure telecommunications facilities must be protected by an intrusion detection system or guarded in accordance with NSTISSI No. 4005, "Safeguarding COMSEC Facilities and Material."

Describe any special security controls in place for unattended secure telecommunications facilities. Information on response time to an alarm, storage of keyed COMSEC equipment and maintenance manuals, procedures for inspection of the facility, emergency procedures, etc., should be addressed in the plan.

19.0 SECURITY OF AUTOMATIC DATA PROCESSING (ADP) SYSTEMS

The regulations of 10 CFR 95.49 state that classified information must not be processed on any ADP systems (e.g., mainframes, mini, micro or personal computer) or LAN unless the system and procedures to protect the classified information have been approved by the NRC. If processing classified information on ADP systems is planned, the facility must submit a plan for NRC approval. Describe the procedures for submitting such security plans and how changes are made to the plans.

Classified data or information may not be processed or produced on an ADP system unless the system and procedures to protect the classified data or information have been approved by the CSA. Approval of the ADP system and procedures is based on a satisfactory ADP security proposal submitted as part of the licensee's, certificate holder's or other person's request for Facility Security Clearance as outlined in 10 CFR 95.15 or submitted as an amendment to its existing Standard Practice Procedures Plan for the protection of classified information. (10 CFR 95.49)

19.1 Justification

Identify the application(s) processing classified data and provide a description of the level of classification (e.g., SECRET, CONFIDENTIAL) and types (e.g., National Security Information, Restricted Data) of data and information to be processed or produced under security cognizance of the NRC. Indicate the probable duration of the ADP activity and relative importance of this activity. Identify the highest classification level of data to be processed and information to be produced.

19.2 Duration and Nature of Activity

Indicate the beginning date and probable duration of this secure ADP activity. In addition, provide an estimate of the percentage of processing time required for handling classified information as compared with unclassified information on the specified ADP system.

19.3 Supplementary Glossary of Terms

Identify and define any special terminology applicable to the secure ADP facility or its ADP system described in this plan which may be system unique or not defined in NSTISSI No. 4009, "National Information Security (INFOSEC) Glossary," or in the "Handbook of INFOSEC Terms (Unified INFOSEC Glossary) copy right 9/96 (or newer) as provided to NSA by the Center for Decision Support of the Idaho State University.

"ADP system" as used in this issuance refers to the interacting of procedures, methods, personnel, and ADP equipment (e.g., mainframes, mini, micro or personal computer, word processor or LANs) to perform a series of data processing operations largely by automated means. This term includes data acquisition systems, networks (local area and world wide) process control systems, minicomputer systems, micro and personal computers in addition to large scale systems and office automation systems.

"ADP center" and "ADP facility" are used synonymously in this issuance and refer to the one or more rooms or a building containing the main elements of one or more ADP systems.

19.4 System Functional Block Diagram

Show the functional interrelationship on a block diagram of all equipment associated with the computer center or LAN, including peripheral equipment, cryptographic equipment, if any, and modems. Include any and all terminals located outside the computer center. Indicate any terminals or networks with which the communications equipment communicates or is planned to communicate with. Provide a brief narrative description, as necessary, to support the system functional block diagram. NOTE: May be combined with Section 18.5.

19.5 Equipment

List nomenclature of all equipment which comprises the secure ADP system, including peripheral equipment, cryptographic equipment, if any, modems and all terminal equipment located outside the facility. Identify the manufacturer's name and the model number of each piece of equipment. Where more than one classified ADP system is joined to another, or a classified ADP system has connectability to an unclassified ADP system or network while not used in classified mode, Section 18.4 requirements must also be satisfied.

19.5.1 Computer System Upgrading/Downgrading Procedures

If the computer system, LAN, or microcomputer is used for the processing of both unclassified and classified data, describe in detail the procedures/adjustments for system, LAN, or microcomputer switch over

between classified and unclassified modes of operation to prevent the compromise of classified data. Include procedures/methods used to disconnect dial-up ports if such a procedure exists for any application.

19.6 Hardware and Software

Describe the security measures incorporated in the ADP hardware (e.g., connector lock boxes, bounds registers) and software (e.g., passwords, programs, access identification, cryptographic methods, specialized subroutines) used in this system to preclude the unauthorized disclosure of classified information or the improper use of the system.

19.6.1 Maintenance Procedures

Describe policies and procedures as to how classified ADP systems are maintained (e.g., internal technicians, cleared contractors).

19.7 System Integrity Study

Specify when an ADP system integrity study or risk analysis will be conducted and submitted to the NRC. If completed, attach a copy to the Security Plan, if not, state when it will be completed and submitted.

19.8 Contingency Plan

If a contingency plan exists with respect to processing classified data, for any/all computer centers, LANs, and microcomputer applications, attach a copy to the security plan. Indicate where in the plan protective measures for classified data are described. If a plan does not presently exist, indicate when it will be submitted to the NRC.

19.9 Personnel Security Clearance

Describe the personnel security measures in effect at the secure ADP facility. Indicate whether all personnel who have access to the ADP facility possess appropriate access authorization (e.g., security clearance) for the highest level of classified data processed or classified information produced by the facility. If not, what precautions are taken to ensure that only properly cleared personnel with a need-to-know are present while work is proceeding on a classified system?

19.10 ADP Security Officer

19.10.1 Selection of ADP Security Officer

Identify an ADP security officer and a necessary alternate(s), at least one of whom will be present during the processing of classified data and information who will ensure that hardware and software security measures are established in each secure ADP center and terminal, and who will monitor the security features of the system.

19.10.2 ADP Security Officer Training

Only properly trained personnel (based on NRC reviewed and accepted training plans and records of individual training completion) may be ADP Security Officers. Should this individual also perform as a COMSEC Custodian or Alternate, he/she must also meet the requirements of 18.6.2.

19.11 Processing of Classified Material

19.11.1 Indication of Classified Information Content

Identify the method of indicating the classification level and category on classified records as displayed and printed, and other classified matter. This should include, but is not limited to, printouts, ribbons, CRT displays, removable mass storage media, and covers for magnetic and paper tapes, and containers. Describe how classified information contained in files and data sets will be identified.

19.11.2 Job Submission and Retrieval

Describe the methods to be used to submit and retrieve classified matter processed by the secure ADP system.

19.11.3 Processing of Classified Data and Information

Include a copy of written instructions for processing classified data and information used by the secure ADP system.

19.12 Facility Security

19.12.1 Description of the Secure ADP Facility

Describe the location of the secure ADP system and discuss the functions and relative locations of adjacent rooms and buildings. Include appropriate building floor plans and plot plans to support this discussion. Indicate whether the secure ADP facility will be established as a Restricted Area, or will be included in a larger Restricted Area. In addition, advise whether it will be a temporary or permanent Restricted Area.

19.12.2 Floor Plans and Drawings

Floor plans and drawings (which must agree with section 18.7.7) shall be identified as follows:

1. Floor plans of the secure ADP facility, showing the locations of all equipment, including all input/output, cryptographic, and telecommunications equipment.

2. Floor plans and an elevation view of the room(s) comprising the secure ADP facility, showing the construction of walls, floor, and ceiling of the room(s).

3. Separate architectural details such as doors, windows, and ducts.

4. Floor plans which indicate the type of facilities and operations in the areas adjacent to and on the floors immediately above and below the secure ADP facility and all measurements between classified and unclassified hardware.

5. Installation drawings wiring diagrams and conduit plans for equipment and lines used for processing or transmitting classified information or data.

19.12.3 Control of Combinations

Describe the method used for controlling (recording and changing) storage repository combinations for the ADP center and ADP terminal areas and the frequency of review by an authorized official. Note any special provisions for controlling the combinations of containers used to store COMSEC documents and materials. Describe the written instructions furnished to ADP personnel and users in this regard.

19.12.4 Intrusion Alarm System/Protective Personnel

Describe the type of intrusion alarm system used to protect the ADP system (including classified media and terminals) and where the alarm annunciates. Specify that the response time of protective personnel who must respond to alarms is less than a maximum of 15 minutes, except in the case of COMSEC documents and material. In such cases, response time is a maximum of 5 minutes.

19.12.5 Access Lists

Discuss the personnel access lists to be used to control entry to the secure ADP facility. Include the functional titles of the individuals who will have access to the facility and their frequency of review by the ADP Security Officer. Give the title of the official who will generate the access lists and the method to be used for developing and maintaining the up-to-date lists.

19.12.6 Authorized User Lists

Provide a list of all functional units considered authorized users of the secure ADP system which are authorized to submit classified jobs or receive classified output. List the functional titles of personnel permitted to operate remote terminals. State the measures which have been taken to preclude unauthorized accessing of classified data or information.

19.12.7 Access by Unlisted Personnel (Visitor Log)

Describe the method of approval of access to the secure ADP facility by persons who are not on the access lists maintained by the secure ADP facility, including cleaning and maintenance personnel. Describe the format of the log, if any, to be maintained for persons who are not on the access lists and require access to the secure ADP facility on a nonroutine basis. Define any requirements for escorts or other means for monitoring such personnel while in the facility.

19.12.8 Personnel Identification System

Describe the means for personnel identification for access to the ADP center or ADP terminal, particularly any specific features that are different from those used for admission to the total facility.

19.12.9 Verification of Security Clearance

Describe briefly the process used in verifying personnel security clearance in connection with access to the secure ADP facility.

19.12.10 Storage

Describe the storage of classified ADP media, punch cards, software used on personal computers, paper or magnetic tapes, printouts, aperture cards, removable mass storage media (including magnetic cartridges and disk packs), and nonremovable mass storage media (including drums and main memory).

19.12.11 Destruction of Printed, Recorded, or Displayed Classified Information or Data

Identify the pertinent types of ADP storage media (e.g., computer printout, magnetic tape, disk drum, magnetic core memory, thin film, and plated wire memories) used or to be used in connection with classified information. Identify the classification level (e.g., SECRET or CONFIDENTIAL) and the type of classified information or data (National Security Information or Restricted Data) stored in each medium. Indicate where, when, and by whom ADP classified information or data is destroyed and the methods of destruction (e.g., paper shredding, a degaussing device or strong permanent magnet, overwriting or any other special method or equipment). Provide the manufacturer's name and model number of any equipment to be considered by the NRC Division of Facilities and Security as approved equipment, and describe the technique used in the destruction process.

19.13 Security Awareness

For computer centers, LANs, or microcomputer processing classified data, describe the security education program to include security orientation and continuing security education for the users of these capabilities, for those who operate the center or LAN equipment and for those who operate the microcomputers processing classified data.

20.0 RETRIEVAL OF CLASSIFIED MATTER FOLLOWING SUSPENSION OR REVOCATION OF ACCESS AUTHORIZATION

Indicate that in the case where the access authorization of an individual is suspended or revoked in accordance with the procedures set forth in part 25 of this chapter, or other relevant CSA procedures, the licensee, certificate holder or other person shall, upon due notice from the Commission of such suspension or revocation, retrieve all classified information possessed by the individual and take the action necessary to preclude that individual having further access to the information.

Describe in detail how this requirement will be carried out. (10 CFR 95.51)

21.0 TERMINATION OF FACILITY SECURITY CLEARANCE

If the need to use, process, store, reproduce, transmit, transport, or handle classified matter no longer exists, the Facility Security Clearance will be terminated. The facility may deliver all documents and materials containing classified information to the Commission or to a person authorized to receive them or destroy all such documents and materials. In either case, the facility shall submit a certificate of non-possession of classified information to the NRC Division of Facilities and Security within 30 days of the termination of the facility clearance.

In any instance where the Facility Security Clearance has been terminated based on a determination of the CSA that further possession of classified matter by the facility would not be in the interest of the national security, the facility shall, upon notice from the CSA, dispose of classified documents in a manner specified by the CSA.

Describe how these requirements will be met. (10 CFR 95.53 (a) and (b))

§73.21 Requirements for the protection of safeguards information.

(a) *General performance requirement.* Each licensee who (1) possesses a formula quantity of strategic special nuclear material, or (2) is authorized to operate a nuclear power reactor, or (3) transports, or delivers to a carrier for transport, a formula quantity of strategic special nuclear material or more than 100 grams of irradiated reactor fuel, and each person who produces, receives, or acquires Safeguards Information shall ensure that Safeguards Information is protected against unauthorized disclosure. To meet this general performance requirement, licensees and persons subject to this section shall establish and maintain an information protection system that includes the measures specified in paragraphs (b) through (i) of this section. Information protection procedures employed by State and local police forces are deemed to meet these requirements.

(b) *Information to be protected.* The specific types of information, documents, and reports that shall be protected are as follows:

(1) *Physical protection at fixed sites.* Information not otherwise classified as Restricted Data or National Security Information relating to the protection of facilities that possess formula quantities of strategic special nuclear material, and power reactors. Specifically:

(i) The composite physical security plan for the nuclear facility or site.

(ii) Site specific drawings, diagrams, sketches, or maps that substantially represent the final design features of the physical protection system.

(iii) Details of alarm system layouts showing location of intrusion detection devices, alarm assessment equipment, alarm system wiring, emergency power sources, and duress alarms.

(iv) Written physical security orders and procedures for members of the security organization, duress codes, and patrol schedules.

(v) Details of the on-site and off-site communications systems that are used for security purposes.

(vi) Lock combinations and mechanical key design.

(vii) Documents and other matter that contain lists or locations of certain safety-related equipment explicity 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.

(viii) The composite safeguards contingency plan for the facility or site.

(ix) Those portions of the facility guard qualification and training plan which disclose features of the physical security system or response procedures.

(x) Response plans to specific threats detailing size, disposition, response times, and armament of responding forces.

(xi) Size, armament, and disposition of on-site reserve forces.

(xii) Size, identity, armament, and arrival times of off-site forces committed to respond to safeguards emergencies.

(xiii) Information required by the Commission pursuant to 10 CFR 73.55 (c) (8) and (9).

(2) *Physical protection in transit.* Information not otherwise classified as Restricted Data or National Security Information relative to the protection of shipments of formula quantities of strategic special nuclear material and spent fuel. Specifically:

(i) The composite transportation physical security plan.

(ii) Schedules and itineraries for specific shipments. (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.)

(iii) Details of vehicle immobilization features, intrusion alarm devices, and communication systems.

(iv) Arrangements with and capabilities of local police response forces, and locations of safe havens.

(v) Details regarding limitations of radio-telephone communications.

(vi) Procedures for response to safeguards emergencies.

(3) *Inspections, audits and evaluations.* Information not otherwise classified as National Security Information or Restricted Data relating to safeguards inspections and reports. Specifically:

(i) Portions of safeguards inspection reports, evaluations, audits, or investigations that contain details of a licensee's or applicant's physical security system or that disclose uncorrected defects, weaknesses, or vulnerabilities in the system. 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, e.g., the Freedom of Information Act (5 U.S.C. 552).

(4) *Correspondence.* Portions of correspondence insofar as they contain Safeguards Information specifically defined in paragraphs (b)(1) through (b)(3) of this paragraph.

(c) *Access to Safeguards Information.* (1) Except as the Commission may otherwise authorize, no person may have access to Safeguards Information unless the person has an established "need to know" for the information and is:

(i) An employee, agent, or contractor of an applicant, a licensee, the Commission, or the United States Government. However, an individual to be authorized access to Safeguards Information by a nuclear power reactor applicant or licensee must undergo a Federal Bureau of Investigation criminal history check to the extent required by 10 CFR 73.57;

(ii) A member of a duly authorized commmittee of the Congress;

(iii) The Governor of a State or designated representatives;

(iv) 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;

(v) A member of a state or local law enforcement authority that is responsible for responding to requests for assistance during safeguards emergencies; or

(vi) An individual to whom disclosure is ordered pursuant to §2.744(e) of this chapter.

(2) Except as the Commission may otherwise authorize, no person may disclose Safeguards Information to any other person except as set forth in paragraph (c)(1) of this section.

(d) *Protection while in use or storage.* (1) While in use, matter containing Safeguards Information shall be under the control of an authorized individual.

(2) While unattended, Safeguards Information shall be stored in a locked security storage container. Knowledge of lock combinations protecting Safeguards Information shall be limited to a minimum number of personnel for operating purposes who have a "need to know" and are otherwise authorized access to Safeguards Information in accordance with the provisions of this section.

(e) *Preparation and marking of documents.* Each document or other matter that contains Safeguards Information as defined in paragraph (b) in this section shall be marked "Safeguards Information" in a conspicuous manner to indicate the presence of protected information (portion marking is not required for the specific items of information set forth in paragraph §73.21 (b) other than guard qualification and training plans and correspondence to and from the NRC). Documents and other matter containing Safeguards Information in the hands of contractors and agents of licensees that were produced more than one year prior to the effective date of this amendment need not be marked unless they are removed from storage containers for use.

(f) *Reproduction and destruction of matter containing Safeguards Information.* (1) Safeguards Information may be reproduced to the minimum extent necessary consistent with need without permission of the originator.

(2) Documents or other matter containing Safeguards Information may be destroyed by any method that assures complete destruction of the Safeguards Information they contain.

(g) *External transmission of documents and material.* (1) Documents or other matter containing Safeguards Information, when transmitted outside an authorized place of use or storage, shall be packaged to preclude disclosure of the presence of protected information.

(2) Safeguards Information may be transported by messenger-courier, United States first class, registered, express, or certified mail, or by any individual authorized access pursuant to §73.21(c).

(3) Except under emergency or extraordinary conditions, Safeguards Information shall be transmitted only by protected telecommunications circuits (including facsimile) approved by the NRC. Physical security events required to be reported pursuant to §73.71 are considered to be extraordinary conditions.

(h) *Use of automatic data processing (ADP) systems.* Safeguards Information may be processed or produced on an ADP system provided that the system is self-contained within the licensee's or his contractor's facility and requires the use of an entry code for access to stored information. Other systems may be used if approved for security by the NRC.

(i) *Removal from Safeguards Information category.* Documents originally containing Safeguards Information shall be removed from the Safeguards Information category whenever the information no longer meets the criteria contained in this section.

[46 FR 51724, Oct. 22, 1981, as amended at 54 FR 17704, Apr. 25, 1989; 59 FR 38899, Aug. 1, 1994]