Standard Practice Procedures Plan
Standard Format and Content for the Protection of Classified Matter for NRC Licensees, Certificate Holder, or Other Activities as the Commission May Determine

Division of Security Operations
U. S. Nuclear Regulatory Commission

July 2011

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 Security Operations at 301-415-7048.

TABLE OF CONTENTS

1.0 PURPOSE 1

2.0 SCOPE 1

3.0 SITE AND FACILITY DESCRIPTION 1
- 3.1 Facility Name and Address 1
- 3.2 Description of Site and Identification of Activity 2
- 3.3 Security Storage Facility 2
  - 3.3.1 Location of Classified Matter 2
  - 3.3.2 Construction Features 2
- 3.4 Classified Mail/Shipping Address 2
- 3.5 Foreign Ownership, Control or Influence (FOCI) 3
- 3.6 Key Personnel 3
- 3.7 Other Agencies Approved Plans 3

4.0 SECURITY ORGANIZATION 3

5.0 TYPE OF CLASSIFIED INFORMATION/MATTER 4
- 5.1 Type of Classified Information/Matter To Be Handled 4
- 5.2 Description of Classified Information/Matter 4

6.0 PERSONNEL SECURITY 4
- 6.1 Requests for NRC Access Authorization 4
- 6.2 Review and Control of NRC Access Authorization Processing 4
- 6.3 Confidentiality of Information 5
- 6.4 Cancellation of NRC Access Authorization Requests 5
- 6.5 Handling of Security Terminations 5
- 6.6 Continued Eligibility for NRC Access Authorization 5
- 6.7 Notification of Grant of Access Authorization 5
- 6.8 Classified Visits 6

7.0 RECORDS MAINTENANCE 6

8.0 PROTECTION OF CLASSIFIED INFORMATION/MATERIAL IN STORAGE 7
- 8.1 Intrusion Alarm Systems 7
  - 8.1.1 Alarm Types 7
  - 8.1.2 Alarm Zones 8
  - 8.1.3 Central Alarm Station 8
  - 8.1.4 Alarm Zone Annunciation 8
  - 8.1.5 Access Mode of Operation 8
  - 8.1.6 Line Security 8
  - 8.1.7 Tamper Protection 9

8.1.8 Emergency Power 9
8.1.9 Local Alarm Annunciation 9
8.2 Protective Personnel 9
8.2.1 General Description 9
8.2.2 Selection 9
8.2.3 Training 9
8.2.4 Qualifications 10
8.2.5 Posts 10
8.2.6 Patrols 10
8.2.7 Communications 10
8.3 Physical Checks 10
8.4 Classified Lock Combinations 10
8.4.1 Records 10
8.4.2 Conditions Under Which Combinations Must Be Changed 11
8.4.3 Records of Combination 11
8.4.4 Selection of Combinations 11
8.4.5 Cautions Regarding Combinations and Authority to Change Combinations 11
8.5 Posted Information 12
8.6 End of Day Security Checks 12
8.7 Unattended Security Container Found Open 12
8.8 Key Control 12

9.0 PROTECTION OF CLASSIFIED MATTER WHILE IN USE 12

10.0 ESTABLISHMENT OF RESTRICTED OR CLOSED AREAS 12

11.0 SECURITY EDUCATION 14

12.0 ACCESS TO MATTER CLASSIFIED AS NATIONAL SECURITY INFORMATION AND RESTRICTED DATA 16
12.1 Access by representatives of the International Atomic Energy Agency or by participants in other international agreements 17

13.0 CLASSIFICATION AND PREPARATION OF DOCUMENTS 18

14.0 EXTERNAL TRANSMISSION OF DOCUMENTS AND MATERIAL 23
14.1 External receipt and dispatch records 25

15.0 AUTHORITY TO REPRODUCE CLASSIFIED INFORMATION 26

16.0 DESTRUCTION OF MATTER CONTAINING NATIONAL SECURITY INFORMATION AND RESTRICTED DATA 26

17.0 REPORTS TO THE NRC 26

18.0 SECURE TELECOMMUNICATIONS 27
18.1 Justification for the Need for Secure Telecommunications 28
18.2 Duration and Nature of Activity 28
18.3 Supplementary Glossary of Terms 28
18.4 Equipment and Media 28
18.5 System Functional Block Diagram 29
18.6 COMSEC 29
18.6.1 COMSEC Accounts 29
18.6.2 COMSEC Custodians and Alternates 29
18.6.3 COMSEC Material Accountability 30
18.6.4 Storage, Transportation, Reproduction, and Destruction of COMSEC Material 30
18.6.5 COMSEC Training 31
18.7 Fixed COMSEC Facilities, Telecommunications Facilities, Secure Communications Centers 31
18.7.1 Physical Security 31
18.7.2 Access Lists 31
18.7.3 Visitor Control 32
18.7.4 Intrusion Alarm System/Protective Personnel 32
18.7.5 Protecting Passwords and Lock Combinations 32
18.7.6 Destruction 32
18.7.7 Floor Plans and Drawings 32
18.7.8 TEMPEST 33
18.7.9 Nonessential Audio Visual Equipment 33
18.7.10 Technical Security Evaluation (TSE) 34
18.7.11 COMSEC Inspections 34
18.7.12 Unattended Secure Telecommunications Facilities 35

19.0 **SECURITY OF AUTOMATIC DATA PROCESSING (ADP) SYSTEMS** 35
19.1 Justification 35
19.2 Duration and Nature of Activity 36
19.3 Supplementary Glossary of Terms 36
19.4 System Functional Block Diagram 36
19.5 Equipment 36
19.5.1 Computer System Upgrading/Downgrading Procedures 37
19.6 Hardware and Software 37
19.6.1 Maintenance Procedures 37
19.7 System Integrity Study 37
19.8 Contingency Plan 37
19.9 Personnel Security Clearance 37
19.10 ADP Security Officer 38
19.10.1 Selection of ADP Security 38
19.10.2 ADP Security Officer Training 38

19.11 Processing of Classified Material 38
19.11.1 Indication of Classified Information Content 38
19.11.2 Job Submission and Retrieval 38
19.11.3 Processing of Classified Data and Information 38
19.12 Facility Security 39
19.12.1 Description of the Secure ADP Facility 39
19.12.2 Floor Plans and Drawings 39
19.12.3 Control of Combinations 39
19.12.4 Intrusion Alarm System/Protective Personnel 40
19.12.5 Access Lists 40
19.12.6 Authorized User Lists 40
19.12.7 Access by Unlisted Personnel (Visitor Log) 40
19.12.8 Personnel Identification System 40
19.12.9 Verification of Security Clearance 41
19.12.10 Storage 41
19.12.11 Destruction of Printed, Recorded, or Displayed Classified Information or Data 41
19.13 Security Awareness 41

20.0 RETRIEVAL OF CLASSIFIED MATTER FOLLOWING SUSPENSION OR REVOCATION OF ACCESS AUTHORIZATION 41

21.0 TERMINATION OF FACILITY SECURITY CLEARANCE 42

STANDARD PRACTICE PROCEDURES PLAN
STANDARD FORMAT AND CONTENT FOR THE PROTECTION OF CLASSIFIED MATTER FOR NUCLEAR REGULATORY COMMISSION LICENSEES, CERTIFICATE HOLDER, OR OTHER ACTIVITIES AS THE COMMISSION MAY DETERMINE

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, or other activities as the Commission may determine. (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 emp1oyee'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 Security Operatons, 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

Security Operations 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 uti1ized 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 at least on an annual basis. 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 Security Operations, 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 Security Operations 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/Date)

Reason_____
Declassify On: _____
(Date/Event/Exemption)
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/Date)
Reason_____
Declassify On: Source Marked "OADR"
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 Security Operations, 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 Security Operations, 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 Security Operations 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 Express Mail and 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(e), 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 Security Operations. 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 Security Operations) 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 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., STE's, STU-IIIs, Secure Cell Phones, 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:

d. 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 Security Operations 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))