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

January 10, 1980

5.59

REGULATORY GUIDE SUBSCRIPTION LIST (DIVISION 5)

Draft Regulatory Guide MP 711-4, "Standard Format and Content for a Licensee Physical Security Plan for the Protection of Special Nuclear Material of Moderate or Low Strategic Significance," was issued for public comment in July 1979. The purpose of the guide is to identify the information needed by the staff in its review of licensees' physical security plans for protection of special nuclear material of moderate or low strategic significance and to provide an acceptable format for its submission. In addition, the guide provides information on the intent of the various provisions of amendments to Part 73 of the Commission's regulations published July 24, 1979, as an aid to the licensee in developing the plan.

Since the draft guide was issued for public comment, the Commission has identified a need for additional clarification of the intent of portions of these amendments. Accordingly, some changes were made in Chapters 1 and 2 of Parts I and II of this guide to fulfill this need. Chapter 1 was expanded to better define the controlled access areas where the material will be used or stored. Chapter 2 was revised to clearly explain what is meant by 73.67(a)(2) "... early detection and assessment of unauthorized access or activities by an external adversary within the controlled access area..." and "... early detection of removal of special nuclear material by an external adversary from a controlled access area." The section in Chapter 2 on intent was expanded to explain how detection devices or procedures could be used to provide early detection against theft of various types of SNM of moderate or low strategic significance.

Comments on regulatory guides are encouraged at all times, but comments on the above changes in Chapters 1 and 2 of Parts I and II will be particularly helpful to the NRC staff in evaluating the need for an early revision to this guide.

Robert B. Minogue

Robert B. Minogue, Director
Office of Standards Development

January 1980

U.S. NUCLEAR REGULATORY COMMISSION

REGULATORY GUIDE

OFFICE OF STANDARDS DEVELOPMENT

Task MP 711-4

REGULATORY GUIDE 5.59

STANDARD FORMAT AND CONTENT FOR A LICENSEE PHYSICAL SECURITY PLAN FOR THE PROTECTION OF SPECIAL NUCLEAR MATERIAL OF MODERATE OR LOW STRATEGIC SIGNIFICANCE

USNRC REGULATORY GUIDES

Regulatory Guides are issued to describe and make available to the public methods acceptable to the NRC staff of implementing specific parts of the Commission's regulations, to delineate techniques used by the staff in evaluating specific problems or postulated accidents, or to provide guidance to applicants. Regulatory Guides are not substitutes for regulations, and compliance with them is not required. Methods and solutions different from those set out in the guides will be acceptable if they provide a basis for the findings requisite to the issuance or continuance of a permit or license by the Commission.

Comments and suggestions for improvements in these guides are encouraged at all times, and guides will be revised, as appropriate, to accommodate comments and to reflect new information or experience. This guide was revised as a result of substantive comments received from the public and additional staff review.

Comments should be sent to the Secretary of the Commission, U.S. Nuclear Regulatory Commission, Washington, D.C. 20555, Attention: Docketing and Service Branch.

The guides are issued in the following ten broad divisions:

1. Power Reactors
2. Research and Test Reactors
3. Fuels and Materials Facilities
4. Environmental and Siting
5. Materials and Plant Protection
6. Products
7. Transportation
8. Occupational Health
9. Antitrust and Financial Review
10. General

Copies of issued guides may be purchased at the current Government Printing Office price. A subscription service for future guides in specific divisions is available through the Government Printing Office. Information on the subscription service and current GPO prices may be obtained by writing the U.S. Nuclear Regulatory Commission, Washington, D.C. 20555, Attention: Publications Sales Manager.

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

INTRODUCTION

The Atomic Energy Act of 1954, as amended, directed the U.S. Atomic Energy Commission (AEC) to regulate the receipt, manufacture, production, transfer, possession, use, import, and export of special nuclear material (SNM) in order to protect the public health and safety and to provide for the common defense and security. The Energy Reorganization Act of 1974 transferred all the licensing and related regulatory functions of the AEC to the Nuclear Regulatory Commission (NRC).

The principal requirements with respect to the physical protection of licensed activities against industrial sabotage and with respect to the physical protection of special nuclear material in transit are found in 10 CFR Part 50, "Domestic Licensing of Production and Utilization Facilities," Part 70, "Domestic Licensing of Special Nuclear Material," Part 73, "Physical Protection of Plants and Materials," and Part 110, "Export and Import of Nuclear Equipment and Materials."

Paragraph 50.34(c) of 10 CFR Part 50 and paragraphs 70.22(g), 70.22(h), and 70.22(k) of 10 CFR Part 70 identify the physical protection information that must be provided in a Physical Security Plan as part of a license application. This plan is required in order for the applicant to demonstrate compliance with the specific physical protection requirements of 10 CFR Part 73 and must be submitted with each application for a license to possess or use SNM (or for a license authorizing transport or delivery of SNM), except for a license to possess, use, or transport less than 10 kg of SNM of low strategic significance, in which case a physical security plan is not required. However, for the protection of SNM of low strategic significance, the licensee is required to meet the requirements of §73.67, "Licensee Fixed Site and In-Transit Requirements for the Physical Protection of Special Nuclear Material of Moderate and Low Strategic Significance," of 10 CFR Part 73.

This regulatory guide describes the information required in the physical security plan submitted as part of an application for a license to possess, use, or transport SNM of moderate strategic significance or 10 kg or more of SNM of low strategic significance and recommends a standard format for presenting the information in an orderly arrangement. This standard format will thus serve as an aid to uniformity and completeness in the preparation and review of the physical protection plan of the license application. This document can also be used as guidance by licensees possessing or transporting less than 10 kg of SNM of low strategic significance in understanding the intent and implementing the requirements of paragraphs 73.67(a), 73.67(f), and 73.67(g) of 10 CFR Part 73.

Aside from providing guidance for the standard format and content of physical security plans, this regulatory guide explains the intent of the various provisions of the regulation. The intent of each requirement is found in the discussion of each subsection and is implicitly provided by outlining alternative systems that could be used to fulfill the requirements. The discussion section and list of alternatives should provide the licensee with the sense of the NRC regulations.

This guide is divided into two parts. Part I, "Special Nuclear Material of Moderate Strategic Significance," provides a standard format for preparing the licensee's security plans and provides guidance to licensees who possess,

use, or transport SNM of moderate strategic significance. Chapters 1 through 6 of Part I apply to applications for a license to possess or use at any fixed site, or at contiguous sites subject to control by the licensee, SNM of moderate strategic significance. Chapters 7 through 11 of Part I apply to applications for authorization to transport or deliver to a carrier for transport SNM of moderate strategic significance.

Part II, "Special Nuclear Material of Low Strategic Significance," provides a standard format for preparing the licensee's security plan for licensees who possess, use, or transport more than 10 kg of SNM of low strategic significance. It also provides guidance to all licensees who possess, use, or transport SNM of low strategic significance. Chapters 1 through 4 of Part II apply to applications for a license to possess or use at any fixed site, or at contiguous sites subject to control by the licensee, more than 10 kg of SNM of low strategic significance. Included in this category are licensees who have nuclear power reactors under construction and are seeking a license to possess nuclear fuel onsite prior to obtaining their operating license. Chapters 5 through 9 of Part II apply to applications for authorization to transport or deliver to a carrier for transport more than 10 kg of SNM of low strategic significance.

Table 1 shows the type and amount of SNM covered in §73.67 of 10 CFR Part 73. It should be noted, as stated in the footnote to Table 1, that (1) plutonium with an isotopic concentration exceeding 80% or more in Pu-238, (2) special nuclear material that is not readily separable from other radioactive material and that has a total external radiation dose rate in excess of 100 rems per hour at a distance of 3 feet from any accessible surface without intervening shielding, and (3) sealed plutonium-beryllium neutron sources totaling 500 grams or less of contained plutonium at any one site or contiguous sites are exempt from the requirements of §73.67 of 10 CFR Part 73.

This guide has been prepared to minimize lost time attributable to incomplete physical security plans and to standardize the review process. The applicant is encouraged to prepare his physical security plan in accordance with this guide and to provide information in each section to support the conclusion that he will be able to operate in accordance with the pertinent regulations. Although conformance with this guide is not required, the format and content presented are acceptable to the NRC staff.

As developments and changes in the nuclear industry occur, the Commission's requirements for information may need modification; revisions to this guide will be made as necessary to accommodate these changes.

Purpose and Applicability

This standard format has been prepared as an aid to uniformity and completeness in the preparation and review of the physical protection section of license applications and to clarify the intent of the regulations. The information this guide contains will help the licensee plan a physical protection system designed to detect the theft of SNM of moderate or low strategic significance. The physical protection subsystems identified are those which will usually be included in a protection system that would normally be capable of meeting the performance requirements of paragraph 73.67(a) of

TABLE 1
CATEGORIES OF SPECIAL NUCLEAR MATERIAL

MATERIAL*	ENRICHMENT	MODERATE STRATEGIC SIGNIFICANCE	LOW STRATEGIC SIGNIFICANCE
1. Plutonium	--	Less than 2,000 g but more than 500 g	500 g or less but more than 15 g
2. Uranium-235	20% or more in U-235 isotope	Less than 5,000 g but more than 1,000 g	1,000 g or less but more than 15 g
	10% or more but less than 20% in U-235 isotope	10,000 g or more	Less than 10,000 g but more than 1,000 g
	Above natural but less than 10%	--	10,000 g or more
3. Uranium-233	--	Less than 2,000 g but more than 500 g	500 g or less but more than 15 g
4. Uranium-235, uranium-233, and plutonium in combination	U-235 portion enriched to 20% or more.	Less than 5,000 g according to the formula: grams = (grams contained U-235) + 2.5 (grams U-233 + grams plutonium) but more than 1,000 g according to the formula: grams = (grams U-235) + 2.0 (grams U-233 + grams plutonium)	1,000 g or less according to the formula: grams = (grams contained U-235) + 2.0 (grams U-233 + grams plutonium) but more than 15 g according to the formula: grams = grams contained U-235 + grams U-233 + grams plutonium.

*The following materials are exempt:

1. Special nuclear material that is not readily separable from the radioactive material and that has a total external radiation dose rate in excess of 100 rems per hour at a distance of 3 feet from any accessible surface without intervening shielding,
2. Plutonium with an isotopic concentration of 80% or more in Pu-238, and
3. Sealed plutonium-beryllium neutron sources totaling 500 grams or less of contained plutonium at any one site or contiguous sites.

10 CFR Part 73. However, it is recognized that at any particular site there may be some subsystems and components not needed or additional ones needed to meet these performance requirements. In these cases, the applicant is encouraged to address in the license application specific departures of subsystems or components from this guide.

The information requested in this guide is the minimum needed for the review of a physical security plan. Additional information may be required for completing the staff review of a particular plan and should be included as appropriate. It is also the applicant's responsibility to be aware of new and revised NRC regulations. The information provided should be up to date with respect to the state of technology for the physical protection techniques and systems that the applicant proposes to use.

In cases where NRC-approved security plans are already in existence and where the measures included therein meet or exceed the requirements of §73.67 of 10 CFR Part 73, the licensee may reference in his proposed security plan those sections of the NRC-approved security plan that are applicable.

Information and procedures delineated in the regulatory guides in Division 5, "Materials and Plant Protection," that are appropriate to certain sections of the physical security plan may be incorporated by reference.

The applicant should discuss his plans and programs with the NRC staff before preparing the application. This discussion should give particular emphasis to the depth of information required for the plan.

Upon receipt of an application, the NRC staff will perform a preliminary review to determine whether the application provides a reasonably complete presentation of the information needed to form a basis for the findings required before issuance of a license. The standard format will be used by the staff as a guideline for identifying the type of information needed. If an application does not provide a reasonably complete presentation of the necessary information, further review of an application will be suspended until this needed information is provided.

Use of the Standard Format

The applicant should follow the numbering system of the Standard Format down to the level of section (e.g., 3.4). Under some circumstances, certain sections may not be applicable to a specific application. If so, this should be clearly stated and sufficient information should be provided to support that conclusion.

The applicant may wish to submit in support of his application information that is not required by regulations and is not essential to the description of the applicant's physical protection program. Such information could include, for example, historical data submitted in demonstration of certain criteria, discussion of alternatives considered by the applicant, or supplementary data regarding assumed models, data, or calculations. This information should be provided as an appendix to the application.

Upon completion of the application, the applicant should use the Table of Contents of the Standard Format as a checklist to ensure that each subject has been addressed.

Style and Composition

A table of contents should be included in each submittal.

The applicant should strive for clear, concise presentation of information. Confusing or ambiguous statements and general statements of intent should be avoided. Definitions and abbreviations should be consistent throughout the submittal and consistent with generally accepted usage.

Wherever possible, duplication of information should be avoided. Thus, information already included in other sections of the applications may be covered by specific reference to those sections.

Where numerical values are stated, the number of significant figures should reflect the accuracy or precision to which the number is known. The use of relative values should be clearly indicated.

Drawings, diagrams, and tables should be used when information may be presented more adequately or conveniently by such means. These illustrations should be located in the section where they are first referenced. Care should be taken to ensure that all information presented in drawings is legible, that symbols are defined, and that drawings are not reduced to the extent that they cannot be read by unaided normal eyes.

Physical Specifications of Submittals

All material submitted in an application should conform to the following physical dimensions of page size, quality of paper and inks, numbering of pages, etc.:

1. Paper Size

   Text pages: 8-1/2 x 11 inches.

   Drawings and graphics: 8-1/2 x 11 inches preferred; however, a larger size is acceptable provided the finished copy when folded does not exceed 8-1/2 x 11 inches.

2. Paper Stock and Ink

   Suitable quality in substance, paper color, and ink density for handling and for reproduction by microfilming.

3. Page Margins

   A margin of no less than one inch is to be maintained on the top, bottom, and binding side of all pages submitted.

4. Printing

   Composition: text pages should be single spaced.

   Type face and style: must be suitable for microfilming.

Reproduction: may be mechanically or photographically reproduced. All pages of the text may be printed on both sides, and images should be printed head to head.

5. Binding

Pages should be punched for looseleaf ring binding.

6. Page Numbering

Pages should be numbered by section and sequentially within the section. Do not number the entire report sequentially. (This entire Standard Format has been numbered sequentially because the individual chapters were too short for sequential numbering within each section to be meaningful.)

7. Format References

In the application, references to this Standard Format should be by part, chapter, and section numbers.

Procedures for Updating or Revising Pages

The updating or revising of data and text should be on a replacement page basis.

The changed or revised portion of each page should be highlighted by a vertical line in the margin opposite the binding margin for each line changed or added. All pages submitted to update, revise, or add pages to the report should show the date of the change. The transmittal letter should include an index page listing the pages to be inserted and the pages to be removed. When major changes or additions are made, pages for a revised table of contents should be provided.

Number of Copies

The applicant should submit the appropriate number of copies of each required submittal pursuant to §70.21, "Filing," of 10 CFR Part 70.

Public Disclosure

The NRC has determined that the public disclosure of the details of physical protection programs is not in the public interest, and such details are withheld pursuant to paragraph 2.790(d) of 10 CFR Part 2. Thus the physical protection section of each application should be submitted as a separate enclosure. Other proprietary and classified information should be clearly identified and submitted in separate enclosures. Each such submission of proprietary information should be accompanied by the applicant's detailed reasons and justifications for requesting exemption from public disclosure as required in paragraph 2.790(b) of 10 CFR Part 2.

PART I

SPECIAL NUCLEAR MATERIAL

OF MODERATE STRATEGIC SIGNIFICANCE

1. USE AND STORAGE AREA AT A FIXED SITE

This chapter provides guidance on meeting the requirements of paragraphs 73.67(d)(1) and (d)(2), which are as follows:

(d)(1) Use the material only within a controlled access area which is illuminated sufficiently to allow detection and surveillance of unauthorized penetration or activities.*

(d)(2) Store the material only within a controlled access area such as a vault-type room or approved security cabinet or their equivalent which is illuminated sufficiently to allow detection and surveillance of unauthorized penetration or activities.*

A controlled access area (CAA) is defined in paragraph 73.2(z) as "any temporarily or permanently established area which is clearly demarcated, access to which is controlled and which affords isolation of the material or persons within it." "Access control" means measures used to allow only specified personnel, materials, and vehicles ingress into and egress from a given area, while "isolation" refers to measures taken to deter persons, materials, or vehicles from entering or leaving a given area through other than established access control points. Thus, a controlled access area includes provisions for both isolation and access control. In some cases, isolation or access control systems may also serve the purpose of aiding in the detection of unauthorized penetration or activities* within the CAA. Therefore these detection-related considerations are alluded to in this chapter.

In the discussion that follows, CAAs intended for use and the possible storage of SNM of moderate strategic significance are discussed separately from those intended solely for the storage of such SNM. Although the requirements for these two different applications of CAA are in most respects similar, it is recognized that the means used to isolate the material and control access may differ markedly for use areas compared with storage areas and therefore warrant separate discussion.

1.1 Area Where Material Is Used [73.67(d)(1)]

Intent

This section discusses CAAs intended primarily for the use of SNM of moderate strategic significance. These may be temporarily established to meet transitory or intermittent SNM use requirements or they may be permanently established. Permanently established CAAs for use of SNM may also be suitable for storage. "Use" means that the material is undergoing processing (e.g. fuel fabrication, irradiation in a reactor, etc.) or utilization of its properties in conjunction with experimental equipment (e.g., research or educational laboratory experiments). Different isolation/access control measures may be used for periods during which the area is occupied versus unoccupied.

---

* Unauthorized activities are those activities deemed by the licensee to be indicative of or contributory to the possible theft of SNM.

Illumination sufficient to allow detection and surveillance of unauthorized penetration or activities within the CAA where the material is used need not require the use of high-intensity lighting throughout the CAA. What is intended is the use of normal lighting sufficiently uniform throughout the CAA to ensure that material or unauthorized personnel cannot be secreted in a darkened area until a time more convenient for the unauthorized removal of the material. For those facilities where experiments must be conducted in a darkened room, the lighting requirement is exempted for as long as is needed provided access control is ensured and the material is accounted for at the end of the experiment.

a. Temporarily Established CAAs

Temporarily established CAAs for the use of SNM need not have permanent barriers at their boundaries. Isolation of the material and persons using the material may be provided by office partitions, cordons, or other devices used to warn passersby of the restricted nature of the area. Access control can be effected through surveillance or supervision of the area by those who are using the SNM and who are responsible for the material. However, the provision of access control through personal supervision is suitable only for those situations in which the size of the CAA and the number of persons to be admitted are sufficiently small and in which the CAA is suitably configured to make such procedures practical.

When material located in a temporarily established CAA is to be left unattended (i.e., because it is impractical to replace the material in a CAA designed for long-term storage of the material), access control and improved isolation for the temporary CAA may be provided to substitute for the discontinued personal supervision over the material. (In addition, provisions must be made for satisfying the monitoring requirement of paragraph 73.67(d)(3).) Improved isolation can sometimes be provided by increasing the penetration resistance of existing barriers (e.g., locking doors and windows, placing the material in a locked drawer or supply room, etc.). Access control may be provided by any of the measures suggested below for permanently established CAAs left unattended; some of these suggestions may be more suitable for temporary use than others. If no suitable barrier is available to provide isolation, material left unattended can be protected by a motion alarm covering the area immediately surrounding the material. This improved detection capability would be considered an acceptable substitute for the rudimentary isolation provided by temporary barricades, cordons, signs, and other less substantial means of isolation that may be used on a temporary basis.

b. Permanently Established CAAs

Permanently established CAAs for the use and temporary storage of SNM of moderate strategic significance would most likely provide isolation for the SNM through the use of permanent barriers. These could consist of fences; gates or freestanding walls for exterior areas; or exterior or interior building walls, locked doors, windows, bars, grillwork; or other barriers for interior areas. Such barriers are not required to meet the more stringent criteria for physical barriers used for the protection of formula quantities

of strategic special nuclear material (SSNM).* However, good security management practice would dictate that the barrier be substantial enough to deter casual passersby from unauthorized penetration. If the barriers are also designed to aid in detection, the criteria for penetration resistance or tamper-indication in accordance with the specific monitoring procedures to be used also apply.

Access control for permanently established CAAs during periods they are occupied can be provided by personal supervision. However, when these areas are unoccupied or when the size, configuration, or numbers of persons intended to be admitted to the area make personal supervision impractical, other means of access control may be called for. Some of the additional access control measures that may be used for permanently established CAAs** in these situations are:

- Stationing of a watchman at CAA access control points,
- Limiting distribution of keys, keycards, or combinations to doors and gates,
- Using a coded badging system to identify authorized personnel at CAA access control points,
- Controlling locked CAA doors and gates by use of remote surveillance (e.g., via intercom or CCTV) by personnel stationed at a centrally located access control facility, or
- Controlling access of personnel, material, and vehicles into CAAs by other means.

It is expected that large facilities will have more complex isolation and access control systems than small facilities in order to achieve comparable levels of protection.

Content

(This section needs to be completed only for CAAs designated exclusively for use of SNM. CAAs designated for both use and storage are to be described as recommended in Section 1.2 of this Standard Format.)

Describe the CAAs designated exclusively for use of the material. Indicate under what conditions CAAs will be established on a temporary basis. For each CAA identified, provide the following information:

1. A description of the area and its features relative to other facility features, showing the normal routes of ingress to each CAA (including a scale diagram).

---

* "Strategic special nuclear material" means uranium-235 (contained in uranium enriched to 20 percent or more in the U-235 isotope), uranium-233, or plutonium.

** Access control requirements for CAAs for the use or storage of SNM of moderate strategic significance are discussed in Chapter 3 of Part I of this guide.

2. Descriptions of physical barriers, cordons, walls, partitions, or other means of providing isolation of the CAA and channelling entry through established access control points into the CAA.

3. The means and criteria used for controlling access into the CAA at established access control points.

4. If more than one CAA is designated, indicate the types of material normally used in each CAA; for temporarily established CAAs, indicate the types of activities normally performed within each area.

5. The lighting level and uniformity of lighting provided to allow detection and surveillance of unauthorized penetration or activities within the CAA or in the immediate vicinity of the CAA.

1.2 Area Where Material Is Stored [73.67(d)(2)]

Intent

Controlled access areas normally used only for storage of SNM are described in this section. Such CAAs may be very limited in size, since they need only contain the material itself, and access to them is expected to be infrequent. Where small amounts of material are involved, the CAA may consist of relatively small containers such as security cabinets, safes, and locked closets or supply rooms.

The same basic isolation and access control* capabilities that apply to CAAs for the use of SNM of moderate strategic significance also apply to CAAs for the storage of this material. However, the CAA for storage is, in addition, specifically required to be equivalent to either an approved security cabinet or a vault-type room. This additional requirement embodies a tradeoff decision to be made by the licensee between the capability for immediate detection of penetration attempts into a vault-type room and the improved penetration resistance likely to be provided by an approved security cabinet.

A vault-type room is defined in paragraph 73.2(o) of 10 CFR Part 73 as "a room with one or more doors, all capable of being locked, protected by an intrusion alarm which creates an alarm upon the entry of a person anywhere into the room and upon exit from the room or upon movement of an individual within the room." The vault-type room can be a locked laboratory, supply room, closet, or other room equipped with a tamper-resistant motion detector alarm system. The motion detector would simultaneously satisfy the monitoring requirement of paragraph 73.67(d)(3) addressed in the next chapter. The expression "equivalent to a vault-type room" means that a piece of equipment (such as a fission chamber, reactor core, or storage rack), even though it does not resemble a "room," may meet the requirement for a storage-type CAA if there is a means of isolation (e.g., a locked grill, inaccessibility beneath water as in a storage pool, intricate and time-consuming procedures required for removal) and it is protected with a tamper-resistant motion detection system. Note that in some cases, material located in such pieces of equipment may be considered in use rather than in storage. In this case,

---

* Access control requirements for CAAs for the use or storage of SNM of moderate strategic significance are discussed in Chapter 3 of Part I of this guide.

whether the material is being personally supervised or not, the requirement for use of a motion detection system to satisfy the monitoring requirement is removed, and other monitoring devices or procedures may be used instead.

When a container equivalent to an approved security cabinet is chosen to satisfy paragraph 73.67(d)(2), the equivalency is based upon the penetration resistance of the container and the difficulty associated with manipulation of the lock. The basic premise used to determine whether such a container may be monitored by procedures or devices other than a motion detector is whether it is unreasonable to expect that an external adversary could penetrate the container in a reasonable amount of time without leaving an indication of the penetration. The amount of time that would be required for penetration without such an indication may be used to govern the frequency of patrols when monitoring procedures are used. An approved security cabinet or its equivalent is one whose design has been certified by the General Services Administration or other nationally recognized standards organization (e.g., ANSI) to afford protection against surreptitious entry and lock manipulation equivalent to that provided by a Class-6 GSA rating or better.

Isolation for CAAs intended only for storage usually will be provided by the penetration resistant features of the perimeter barriers or container walls of the CAA. The level of penetration resistance of such barriers is not required to meet the more stringent criteria for physical barriers used to protect formula quantities of strategic special nuclear material (SSNM). Rather, the physical barriers or container walls of the CAA are intended only to deter penetration by unauthorized persons and to aid detection by providing an indication of forced penetration.

In determining the level of isolation/access control required for such CAAs, the time required for extricating SNM from its storage location in relationship to the licensee's time of detection and assessment may be taken into account (e.g., spent fuel assemblies stored in spent fuel storage pools or fuel residing in nonpower reactor cores).

Examples of typical CAAs where special nuclear material of moderate strategic significance may be stored are:

1. Vault. A structure that satisfies the definition for a vault as stated in paragraph 73.2(n) would provide more than adequate isolation protection.

2. Approved Security Cabinets. Those cabinets that are designed to provide delay and resistance against surreptitious entry and lock manipulation.

3. Reactor. Reactors that are so designed that removal of material is difficult.

4. Vault-Type Room. Some typical vault-type rooms where materials are stored and protected with a motion detector are storage pools, a room containing in-process storage racks, and laboratories where material is left unattended. In all cases, movement in the near vicinity of the material or of the material itself generates an alarm signal.

5. Locked Laboratories, Supply Rooms. These areas must be sufficiently penetration resistant to afford a means of isolation/access control and permit the proper functioning of the system for monitoring the storage area as required by paragraph 73.67(d)(3) of the rule as described in Part I, Chapter 2.

The illumination level required for the CAA should be sufficiently uniform and bright (a) in the case of a security cabinet, to detect penetration of or tampering with the CAA containment or (b) in the case of a vault-type room or its equivalent, to detect unauthorized penetration of or activities within the CAA .

Content

Describe the CAAs where the material will be stored and, in some cases, used. For each such CAA, provide the following information:

1. A description of the area and its features relative to other facility features showing the access control points for the CAA (including a scale diagram).

2. The isolation system such as physical barriers, container walls, or other features which demarcate the perimeter of the CAA and channel entry only through established access control points.

3. The means and criteria used for controlling access to the CAA at established access control points.

4. If more than one CAA is designated for the storage of the material, the types of material normally to be stored in each area.

5. The lighting level and uniformity of lighting provided to allow detection and surveillance of unauthorized penetration or activities within the CAA, or in the immediate vicinity of the CAA (where security cabinets are used).

2. DETECTION DEVICES AND PROCEDURES AT A FIXED SITE

This chapter provides guidance for meeting the requirement of paragraph 73.67(d)(3), which is as follows:

(d)(3) Monitor with an intrusion alarm or other device or procedures the controlled access areas to detect unauthorized penetrations or activities.

The purpose of this monitoring activity as stated in paragraph 73.67(a)(2) is to provide "early detection and assessment of unauthorized access or activities by an external adversary within the controlled access area..." and "early detection of removal of special nuclear material by an external adversary from a controlled access area." This should be done to achieve the objective of minimizing the possibilities for unauthorized removal of special nuclear material "consistent with the consequences of such actions," as stated in paragraph 73.67(a) of the effective rule. Thus the earliness of detection afforded by the licensee's physical protection system may vary depending upon the nature and quantity of the material susceptible to unauthorized removal. Further discussion of the earliness of detection required for possible thefts of different types and quantities of special nuclear material of moderate strategic significance is provided in Section 2.1.

2.1 Earliness of Detection [73.67(a)]

Determination of early detection of unauthorized access, activities, or removal of special nuclear material from controlled access areas will be based on an assessment of the magnitude of the consequences associated with possible misuse of the type and quantity of material that could be removed in a given theft attempt. For special nuclear material of moderate strategic significance, two distinct cases are considered:

1. Theft of strategic special nuclear material (SSNM).*

2. Theft of low-enriched uranium (LEU).**

Thefts from a single facility of SSNM in quantities of moderate strategic significance are limited by definition to quantities that could not be used to construct a nuclear explosive device; thefts of similar quantities of material from several different facilities could, however, lead to the accumulation of an aggregate quantity that would permit such illicit use. (The consequences of a single theft of such material would have minimal impact on the public health and safety). Therefore, detection of such thefts is required sufficiently early to ensure early notification to the NRC so that the NRC in turn can notify other licensees of the need to implement appropriate responses to prevent the accumulation by a single adversary of a formula quantity of material through multiple thefts from different facilities. The NRC believes that there are detection systems and procedures

---

* In this case, Strategic Special Nuclear Material means all SNM of moderate strategic significance other than low-enriched uranium.

** Low-enriched uranium is uranium enriched above natural percentages but less than 20% in the U-235 isotope.

that would allow the licensee to detect a theft of SSNM within approximately two hours.

The criteria for early detection of thefts of LEU enriched to more than 10%, but less than 20%, in the isotope U-235 are the same as for thefts of LEU in quantities comprising SNM of low strategic significance. The reader should refer to Part II of this guide for information regarding appropriate monitoring procedures to achieve early detection for such material.

2.2 Detection Through Monitoring of Controlled Access Areas [73.67(d)(3)]

Intent

Licensees possessing quantities of SNM of moderate strategic significance can provide a monitoring system capable of detecting a theft of material within approximately two hours of the actual removal of the material. Either detection devices or security procedures may be used to help detect unauthorized activities or penetration of CAAs. Most of the sites at which this material is stored or used are likely to be small research-oriented facilities such as non-power reactors and educational institutions. At such facilities there are likely to be relatively small quantities of SNM available, and authorized access to it may be infrequent.

Detection devices such as interior motion detector systems, balanced magnetic switches, etc. could be used to monitor such relatively small CAAs, where the number of established access control points is very limited.

Security procedures may also be used to protect against thefts of quantities of SNM of moderate strategic significance because watchman patrols inherently allow unguarded intervals during which an external adversary could conceivably obtain access to the CAA, remove a small quantity of material, and leave before being discovered. The inspection procedure may (a) be sufficiently frequent to ensure that an external adversary could not complete a successful theft of the material during the unguarded intervals, (b) provide for an indication of the CAA barrier having been tampered with (as with a seal or by observation of damage done to the barrier), or (c) provide for an item count inventory or other accounting for the material as part of the inspection. Some examples are given below:

- After having left material unattended in an experimental setup in a classroom used as a temporary CAA, the instructor returns after several hours and verifies that the material is still in place.

- A small quantity of material is stored in a security cabinet for several months at a time without authorized access. Every two hours a watchman comes around to inspect the cabinet to ensure that the lock is secure and the cabinet has not been tampered with. If a lock is used that is not designed to be resistant to surreptitious and forced entry, the watchman also inspects a tamper-indicating seal to verify that the container has not been tampered with.

- During times a non-power reactor is left unattended, a watchman comes around every two hours and checks that none of the fuel elements have been removed by unauthorized persons. If he encounters a

person working during off-hours in the vicinity of the non-reactor, he asks for appropriate identification.

- While a non-power reactor is being used, the supervisor ensures that he or his designee is not away from the reactor for a period longer than thirty minutes or a period he estimates would be minimally required for a person to obtain fuel elements in the core that are not self-protecting by virtue of their having been sufficiently irradiated.

- During periods when excess fuel is left unattended in a storage closet at a non-power reactor facility, an alarm system is activated that would annunciate if anybody tried to penetrate the closet without proper authorization.

During periods when the material is being used under the direct supervision of authorized personnel, the monitoring requirement may be satisfied by virtue of the continuous surveillance exercised by such personnel.

Content

For each of the CAAs designated for the protection of SNM of moderate strategic significance, provide the following information regarding the measures taken to fulfill the monitoring requirement of paragraph 73.67(d)(3):

1. Describe any devices employed by specifying the type of device, its installed location, the type and location of annunciation, the intended area of coverage, and the tamper-resistant features. Refer, if desired, to existing filed security plans or NRC-published guidance or NUREG series documents.

2. Describe any procedures employed to monitor the CAA or portions thereof, including the categories of persons who will execute the procedures, the frequency of inspections or rounds of patrol, the basis for the determination of such frequencies, and the occasions when the procedures are intended to be implemented. Indicate, also, the features of the CAA (e.g. barriers, locks, seals, etc.) that will affect the way the procedures are used.

3. Explain how the combination of procedures and devices used to monitor each CAA meets the criteria for early detection of theft by an external adversary relative to the type of material found in each CAA.

3. ACCESS CONTROL AT A FIXED SITE

This chapter provides guidance on meeting the requirements of paragraphs 73.67(d)(4), (d)(5), (d)(6), (d)(7), and (d)(10), which are as follows:

(d)(4) Conduct screening prior to granting an individual unescorted access to the controlled access area where the material is used or stored, in order to obtain information on which to base a decision to permit such access,

(d)(5) Develop and maintain a controlled badging and lock system to identify and limit access to the controlled access areas to authorized individuals,

(d)(6) Limit access to the controlled access areas to authorized or escorted individuals who require such access in order to perform their duties,

(d)(7) Assure that all visitors to the controlled access areas are under the constant escort of an individual who has been authorized access to the area,

(d)(10) Search on a random basis vehicles and packages leaving the controlled access areas.

An access control system is one that controls access to or egress from a CAA through normal routes for personnel, materials, or vehicles.

3.1 Preauthorization Screening [73.67(d)(4)]

Intent

The intent of the requirement for preauthorization screening is to ensure that the licensee will have sufficient knowledge of an individual to determine his reliability and need for access prior to granting him authorized access to the CAA where the material is used or stored. The selection of procedures for conducting this examination and the criteria he employs to make his judgments are the responsibility of the licensee and, of course, should be consistent with all local, State, and Federal laws and regulations regarding the protection of the privacy and other rights of the individual. The screening process may be conducted in the same manner as other investigations customarily conducted by potential employers for similarly sensitive positions. There is no requirement for the licensee to arrange for an NRC clearance or similar clearance from any other government organization. Examples of procedures and criteria that may be employed in the screening process include holding or having recently held a government-sanctioned clearance; examination of past employment or educational records (to determine any unsatisfactory employment or school actions or incidents that would indicate any unreliability or previous breaches of trust between the individual and his employer); endorsements or references from previous employers, teachers, or colleagues that would support a decision for granting access or that would attest to the trustworthiness and reliability of the individual; and consideration of the individual's present employment record indicating demonstrated trustworthiness and reliability over an extended period of

employment with the licensee. (This may be considered in the nature of "grandfathering.")

Content

Describe the procedures and criteria that will be used for obtaining sufficient information prior to making a decision on granting unescorted access authorization to an individual to CAAs where the material is used or stored. Identify the types of individuals who will be screened (e.g., process engineers, supervisory personnel, professors, instructors, graduate students) and who will perform the screening process.

3.2 Badging System [73.67(d)(5)]

Intent

The purpose of the badging system is to facilitate the identification of authorized individuals and the control of access to or within the CAA where the material is used or stored. Information on the badge should be such that it is possible to clearly distinguish personnel authorized for access to the CAAs from those requiring an escort. Information on the badge should also uniquely identify the individual possessing the badge. This personalized information can be obtained through the use of photographs, personal vital statistics, signatures, or any means the licensee may wish to use that will uniquely identify the individual.

Content

Describe the badging system used to facilitate control of access to the CAAs. This description should include:

1. The size, shape, color, material, and construction of badges.

2. The distinguishing features of the badge that identify authorized individuals from escorted individuals.

3. How the badges will be used for controlling access. (For example, will all individuals be checked prior to entering the CAAs, will periodic checks be made of individuals within a CAA to determine if they are authorized or under escort, or will the badge itself permit authorized entrance, e.g., a card key.)

4. The system used for issuing, controlling, and accounting for the badges.

3.3 Lock System [73.67(d)(5)]

Intent

Locks used to control access to CAAs should be resistant to manipulation or picking and should not be mastered. Examples of typical lock systems that fit this description are three-position dial-type combination locks, six-pin key locks, and card-key lock systems. The procedures for assigning keys and combinations to individuals is an integral part of the lock system and should be designed to ensure that only authorized personnel have access

to such items. Locks and combinations should be changed when information is obtained that the lock system may have been compromised. Further information may be obtained in Regulatory Guide 5.12, "General Use of Locks in the Protection and Control of Facilities and Special Nuclear Material."

Content

Describe the locking system used to control access to the CAAs where material is used and stored. This description should include locations of all locks included in the system by type of lock, the pick-resistant and manipulation-resistant characteristics of each lock type used, personnel responsible for issuing keys or combinations and changing combinations or locks, criteria for changing combinations or locks, personnel authorized to be given keys or combinations, and descriptions of types of locks used (references may be made to Regulatory Guide 5.12 for this purpose).

3.4 Personnel Entry Control System [73.67(d)(6)]

Intent

The success of other access control system components, such as preauthorization screening, badging, and lock control, is dependent upon effective control of personnel access into the CAA. Physical access may be controlled in a number of different ways depending upon the actual configuration of the CAA and other site specific factors. Some examples of these alternatives are:

1. Control by Authorized Person. If the area to be controlled is sufficiently small and free of obstructions, an authorized person performing other activities in a CAA may effect physical access control by monitoring entry of unauthorized persons into the area. A sign posted at the entrance would help deter casual passersby. A typical application of this approach would be the case of a laboratory instructor conducting a class in which he is familiar with each of his students and could easily recognize unauthorized persons not in the class.

2. Card-Key, Cipher, Combination, or Key-Lock Control System. A more sophisticated hardware-oriented system involves the use of a card-key, cipher, combination, or key-lock system. Physical access control in this case consists of the use of physical barriers to deter unauthorized persons. A limited number of entrances that are controlled by authorized personnel using a card key, cipher, combination, or key are provided. This system may be more useful when larger numbers of authorized personnel who would not necessarily be familiar with one another need to share the use of the CAA.

3. Control by Security Organization. If security organization personnel are available, physical access control may be accomplished by stationing a person at the entrance to the CAA to check identification and allow only authorized persons into the CAA. This alternative may be unjustifiably expensive unless the security organization member's salary can be justified on other grounds as well. A variation of this system requires persons seeking entrance to the CAA to obtain a key from a properly designated person or security organization for each use.

Content

Describe the system for limiting physical access to each CAA identified in Sections 1.1 and 1.2 of Part I to authorized personnel or those escorted by authorized personnel. Include in this description the names or titles of individuals granting access authorizations, the criteria to be used in granting authorizations, and the procedures used to ensure that only authorized or properly escorted persons are allowed access to the CAA. Reference can be made to Sections 3.1, 3.2, 3.3, 3.5, and 3.6 of this chapter as they apply to this section for the description of locks, barriers, or other hardware that are used to control access.

3.5 Escort System [73.67(d)(7)]

Intent

The requirement that an escort system be established is in recognition of the fact that the licensee may wish to allow access to certain persons or classes of persons on a temporary or infrequent basis or on short notice, thus making the routine process for granting access authorizations impractical or inexpedient. Typical arrangements for escorted access may include escorts for maintenance or repair personnel, laboratory classes, public tours, guests, and visitors as required.

Content

Describe the system that will be used to escort individuals in the CAAs. In his security plan, the licensee should ensure that only properly authorized individuals will be allowed to escort individuals. This description should include:

1. Criteria to be used for granting escorted access,

2. Criteria to be used for escorting others,

3. Procedures for escorting individuals into CAAs (e.g., students under supervision of lab instructor, public tours),

4. The number of escorted individuals per escort, and

5. The responsibilities of the escort (e.g., periodic surveillance of all individuals under escort, accounting for all material prior to leaving the CAA, remaining in general area during the time unauthorized individuals are present).

3.6 Search [73.67(d)(10)]

Intent

The primary intent of the search requirement is to deter and possibly detect attempted thefts of SNM. The search procedures developed by the licensee should take into consideration the environs where the material is used or stored, the physical characteristics of the material itself, and the frequency of accounting for the material. In some cases, this will

require that all vehicles and packages leaving the CAAs be searched in a random manner. The frequency of random searches should be determined by the ease with which the material can be stolen and the length of time it would take to detect a theft. In other cases, only packages that equal or exceed the size of the material being used or stored would have to be searched, taking into consideration the difficulty with which the material could be broken into smaller more easily concealed parts.

Content

Describe the system to be used for randomly searching vehicles or packages that leave the CAA. Include in the description information as to:

1. The scope of the search. This should identify the criteria that will be used for searching vehicles and packages (e.g., whether all packages and vehicles are subject to search or just those packages or vehicles that are larger than the smallest configuration of material being used or stored).

2. The randomness of the search. The scheme for selecting the packages or vehicles to be searched should be identified (e.g., subjecting each package or vehicle to a search, using a random number generator for determining whether a candidate package or vehicle is to be searched, searching a minimum percentage of all packages or vehicles leaving the CAA each day).

4. SECURITY ORGANIZATION AT A FIXED SITE

This chapter provides guidance on meeting the requirements of paragraph 73.67(d)(8), which states:

(d)(8) Establish a security organization or modify the current security organization to consist of at least one watchman* per shift able to assess and respond to any unauthorized penetrations or activities in the controlled access areas.

Intent

The intent of this requirement is to ensure that, in the event of a security incident, someone will be available to assess alarms or other unauthorized penetrations or activities and, if warranted, notify the NRC, the local law enforcement authorities, and the responsible person in licensee management. Early detection and notification of any missing material will help facilitate its prompt recovery. In some cases, the licensee may assign additional duties to members of the security organization where procedure-oriented options are chosen to satisfy physical protection requirements (e.g., periodic patrols and inspections of CAAs for storage of SNM). Security organization members are not required to be fully dedicated full-time employees of the licensee. They may include unarmed campus security personnel (watchmen), contract guards, members of the local law enforcement agency (if sufficiently close to the site), etc. No formal or comprehensive training program is required for security organization personnel. However, the licensee should be prepared to demonstrate that each security person understands the particular duties assigned to him and is fully qualified and trained to perform them.

Content

Describe the security organization that will be responsible for assessing and responding to security incidents. Indicate the other responsibilities of the security organization such as:

1. Conducting periodic physical security checks of CAAs,

2. Maintaining liaison with the local law enforcement agency,

3. Notifying the local law enforcement agency of any unauthorized penetrations or activities in the CAAs, and

4. Notifying licensee management of any unauthorized penetrations or activities in the CAAs.

---

* A "watchman" is defined in paragraph 73.2(d) of 10 CFR Part 73 as "an individual, not necessarily uniformed or armed with a firearm, who provides protection for a plant and the special nuclear material therein in the course of performing other duties."

5. COMMUNICATIONS AT A FIXED SITE

This chapter provides guidance on meeting the requirements of paragraph 73.67(d)(9), which states:

(d)(9) Provide a communication capability between the security organization and appropriate response force.

Intent

The intent of this regulation is to ensure that a communication capability exists between the licensee and the designated response force. It is implied that, prior to setting up a communication capability, procedures and responsibilities will have been established between the response force and the licensee. (See Chapter 6, "Response Procedures," of Part 1.) The type of communication system chosen by a licensee should:

1. Provide for full duplex voice communication capability,

2. Be easily accessible to the licensee's security organization, and

3. Be reliable and available for immediate use at any time.

Some communication systems that would provide these capabilities are a dedicated telephone system, a non-dedicated public telephone system, radio, or any combination thereof.

Content

Describe the communication system that is used between the security organization and the appropriate response force. This description should include information on:

1. Type of communication system,

2. Location of voice terminals in relationship to CAAs,

3. Availability of communication system on a 24-hour basis, and

4. Reliability of communication system.

6. RESPONSE PROCEDURES AT A FIXED SITE

This chapter provides guidance on meeting the requirements of paragraph 70.67(d)(11), which states:

(d)(11) Establish and maintain response procedures for dealing with threats of thefts or thefts of such materials.

Intent

The intent of this regulation is to help the licensee to identify those security incidents that could result in the loss of SNM of moderate strategic significance and to develop response procedures to prevent or reduce the likelihood of such a loss. Some types of incidents that should be considered and for which response procedures should be developed are:

1. Situations that could possibly lead to theft of SNM (e.g., civil strife),

2. Discovery that the security system has been breached, and

3. Discovery that some SNM is missing.

Content

Identify those events for which response procedures will be developed. Also, describe the type of response to be accomplished for each event identified and the duties and responsibilities of the security organization and management involved in the response. Ensure that the NRC will be notified immediately in the event of theft or attempted theft of the material. Describe what local law enforcement assistance is available, their response capabilities, and any agreements made with them to respond in the case of theft of the material.

7. MATERIAL TRANSPORTATION REQUIREMENTS

This chapter provides guidance on meeting the requirements of paragraph 73.67(e)(1), which are as follows:

(e)(1) Each licensee who transports, exports, or delivers to a carrier for transport special nuclear material of moderate strategic significance shall:

(i) Provide advance notification to the receiver of any planned shipments specifying the mode of transport, estimated time of arrival, location of the nuclear material transfer point, name of carrier and transport identification,

(ii) Receive confirmation from the receiver prior to the commencement of the planned shipment that the receiver will be ready to accept the shipment at the planned time and location and acknowledges the specified mode of transport,

(iii) Transport the material in a tamper-indicating sealed container,

(iv) Check the integrity of the containers and seals prior to shipment, and

(v) Arrange for the in-transit physical protection of the material in accordance with the requirements of paragraph 73.67(e)(3) of this part unless the receiver is a licensee and has agreed in writing to arrange for the in-transit physical protection.

7.1 Advance Notification [73.67(e)(1)(i)]

Intent

The intent of this paragraph is to require the shipper to preplan the transportation of material and inform the receiver of his plans prior to shipment. This is the first of the several transportation requirements that will allow the receiver to take delivery of the material as planned or to help ensure traceability of any missing material.

Content

The licensee should ensure in his security plan that, prior to each shipment of material, the receiver will be notified of the impending shipment and provided the following types of information:

1. Mode of transport (e.g., truck, plane, train, or ship),

2. Estimated time of arrival,

3. Location where material is to be transferred to receiver,

4. Name of carrier, and

5. Transport identification (e.g., truck, train, or flight number; ship name).

7.2 Receiver Confirmation [73.67(e)(1)(ii)]

Intent

The intent of this requirement is that, prior to shipment, the shipper will be assured that the receiver is ready to accept the shipment at the planned time and location and has acknowledged the mode of transport.

Content

Describe what procedures will be used to ensure that shipment of material does not take place until the receiver acknowledges the planned shipment and mode of transport and states that he will be ready to accept the shipment at the planned time and location.

7.3 Container [73.67(e)(1)(iii)]

Intent

The intent of this requirement is to provide a mechanism or system that will help the receiver detect any tampering with the material's container that may have occurred during shipment. Regulatory Guide 5.15, "Security Seals for the Protection and Control of Special Nuclear Material," provides guidance in this area. Requirements for containers are contained in 10 CFR Part 71, and a summary report on approved containers is contained in NUREG-0383.* If the material is shipped in an exclusive-use carrier, it is acceptable to seal the carrier itself rather than each individual SNM container.

Content

Describe the types of seals that will be used to monitor the material's container during transport.

7.4 Inspection [73.67(e)(1)(iv)]

Intent

The intent of this paragraph is to require the shipper to check the integrity of the material container's seals just prior to shipment so that he can be assured that they have not been compromised. Then, upon receipt of the shipment, if the receiver discovers that the container's integrity has been compromised and the material is missing, the scope of the recovery operation can focus on the transportation route.

Content

Describe the procedures to be used to ensure that the integrity of the containers or seals is checked just prior to shipment.

---

* Copies of NUREG-0383, "Directory of Certificates of Compliance for Radioactive Materials Packages," may be obtained from the National Technical Information Service, Springfield, Virginia 22161.

7.5 Responsibility for In-Transit Physical Protection [73.67(a)(1)(v)]

Intent

The intent of this paragraph is to make clear that the licensee shipping the material is responsible for arranging for the physical protection of the material in transit if the receiver is not a licensee. If both the shipper and receiver are licensees, the shipper may allow the receiver to accept this responsibility wholly or in part, provided there is appropriate documentation specifying their respective responsibilities. Where no such documentation exists, both the shipper and receiver are held jointly responsible. (See Section 8.3 in the next chapter.)

Content

In his security plan, the shipper should either acknowledge responsibility for the in-transit physical protection of SNM of moderate strategic significance or ensure that a written agreement from the receiver licensee has been received in which the receiver accepts either full responsibility or shared responsibility for the in-transit physical protection of this material in accordance with paragraph 73.67(e)(3) of 10 CFR Part 73.

8. RECEIVER REQUIREMENTS--TRANSPORTATION

This chapter provides guidance on meeting the requirements of paragraph 73.67(e)(2), which are as follows:

(e)(2) Each licensee who receives special nuclear material of moderate strategic significance shall:

(i) Check the integrity of the containers and seals upon receipt of the shipment,

(ii) Notify the shipper of receipt of the material as required in Section 70.54 of Part 70 of this chapter, and

(iii) Arrange for the in-transit physical protection of the material in accordance with the requirements of paragraph 73.67(e)(3) of this part unless the shipper is a licensee and has agreed in writing to arrange for the in-transit physical protection.

8.1 Inspection [73.67(e)(2)(i)]

Intent

This requirement is intended to determine whether the material's container has been compromised enroute and whether any material has been removed so that immediate recovery procedures can be initiated if required.

Content

Describe the procedures to be used to ensure that the integrity of the containers and seals will be checked upon receipt of the shipment of material.

8.2 Notification [73.67(e)(2)(ii)]

Intent

This requirement is intended to:

1. Ensure that knowledge of the current location of all SNM is available, and

2. Formally inform the shipper that the material has been received.

Content

Ensure that a completed copy of standard Form NRC-741, "Nuclear Material Transaction Report," will be sent to the shipper within 10 days of receiving a shipment of material as required in §70.54 of 10 CFR Part 70.

8.3 Responsibility for In-Transit Physical Protection [73.67(e)(2)(iii)]

Intent

The intent of this paragraph is to make clear that the licensee receiving the material is responsible for arranging for the physical protection of the material in transit if the shipper is not a licensee. If both the shipper and receiver are licensees, the receiver may allow the shipper to accept this responsibility either wholly or in part provided there is appropriate documentation specifying their respective responsibilities. Where no such documentation exists, both the shipper and receiver are held jointly responsible. (See Section 7.5 in the preceding chapter.)

Content

In his security plan, the receiver should either acknowledge responsibility for the in-transit physical protection of SNM of moderate strategic significance or ensure that a written agreement from the shipper has been received in which the shipper accepts either full responsibility or shared responsibility for the in-transit physical protection of this material in accordance with paragraph 73.67(e)(3) of 10 CFR Part 73.

9. IN-TRANSIT PHYSICAL PROTECTION REQUIREMENTS

This chapter provides guidance on meeting the requirements of paragraph 73.67(e)(3), which are as follows:

(e)(3) Each licensee, either shipper or receiver, who arranges for the physical protection of special nuclear material of moderate strategic significance while in transit or who takes delivery of such material free on board (f.o.b.) the point at which it is delivered to a carrier for transport shall:

(i) Arrange for a telephone or radio communications capability, for notification of any delays in the scheduled shipment, between the carrier and the shipper or receiver,

(ii) Minimize the time that the material is in transit by reducing the number and duration of nuclear material transfers and by routing the material in the most safe and direct manner,

(iii) Conduct screening of all licensee employees involved in the transportation of the material in order to obtain information on which to base a decision to permit them control over the material,

(iv) Establish and maintain response procedures for dealing with threats of thefts or thefts of such material,

(v) Make arrangements to be notified immediately of the arrival of the shipment at its destination, or of any such shipment that is lost or unaccounted for after the estimated time of arrival at its destination, and

(vi) Conduct immediately a trace investigation of any shipment that is lost or unaccounted for after the estimated arrival time and report to the Nuclear Regulatory Commission as specified in §73.71 and to the shipper or receiver as appropriate. The licensee who made the physical protection arrangements shall also immediately notify the Director of the appropriate Nuclear Regulatory Commission Inspection and Enforcement Regional Office listed in Appendix A of the action being taken to trace the shipment.

It is not the intent of these paragraphs to require that the responsible licensee for shipping SNM of moderate strategic significance ship the material under armed escort or in a specially designed carrier.

9.1 Communications [73.67(e)(3)(i)]

Intent

The primary intent of this requirement is to ensure that the carrier will notify the shipper or receiver of any changes in plans or delays in the scheduled arrival of a shipment to its destination due to mechanical breakdown, adverse environmental conditions, public disorders, etc. The

shipper or receiver can then decide whether or not to initiate response procedures. It is not the intent of this regulation to require periodic check-in. Public telephone or full duplex voice radio are acceptable methods for meeting the intent of this requirement.

Content

Describe the type of communication system and procedures to be used by the carrier of SNM of moderate strategic significance for notifying the shipper or receiver of any change in plans or delays in arrival.

9.2 Minimum Transit Times [73.67(e)(3)(ii)]

Intent

This requirement is intended to have the shipper or receiver make a reasonable effort to ship the material by the fastest and most direct method possible. It is not intended to require exclusive-use carriers or expensive modes of travel.

Content

Describe the procedures and considerations that apply in the transportation planning process to ensure that a determined effort will be made to minimize transit times.

9.3 Preauthorization Screening [73.67(e)(3)(iii)]

Intent

The intent of the requirement for preauthorization screening is to ensure that the licensee will have sufficient knowledge of an individual to determine his reliability and need for access prior to granting him authorized access to the material in transit. The selection of procedures for conducting this examination and the criteria he employs to make his judgements are the responsibility of the licensee and, of course, should be consistent with all local, State, and Federal laws and regulations regarding the protection of the privacy and other rights of the individual. The screening process may be conducted in the same manner as are other investigations customarily conducted by potential employers for similarly sensitive positions. There is no requirement for the licensee to arrange for an NRC clearance or similar clearance from any other government organization. Examples of procedures and criteria that may be employed in the screening process include holding or having recently held a government-sanctioned clearance; examination of past employment records (to determine any unsatisfactory employment or incidents that would indicate any unreliability or previous breaches of trust between the individual and his employer); endorsements or references from previous employers or colleagues that would support a decision for granting access or that would attest to the trustworthiness and reliability of the individual; and consideration of the individual's present employment record indicating demonstrated trustworthiness and reliability over an extended period of employment with the licensee. (This may be considered in the nature of "grandfathering.")

Content

Describe the procedures that will be used for obtaining sufficient information prior to making a decision on granting unescorted access authorization to those licensee employees who will be directly involved in the transportation or in the planning and movement control of the material. Identify by title or name those employees who will be screened and those who will perform the screening process.

9.4 Response Procedures [73.67(e)(3)(iv)]

Intent

The intent of this regulation is to help the licensee to identify those transportation incidents for which he might expect to be notified and that might affect the security of the SNM in transit and to plan response procedures for such situations. For example, if the shipper is informed by the carrier that adverse weather conditions have temporarily prevented further progress of the shipment, the licensee should inform the receiver of a new estimated time of arrival.

Content

Identify those events for which response procedures will be developed. Also, describe types of response to be accomplished for each event identified and the duties and responsibilities of members of the security organization and management for dealing with the response. Ensure that the NRC will be notified immediately in the event of theft or attempted theft of the material.

9.5 Notification [73.67(e)(3)(v)]

Intent

The intent of this requirement is to ensure that the licensee responsible for the physical protection of SNM in transit will have a firm basis for deciding whether or not to initiate response procedures in the event a shipment becomes overdue or is lost.

Content

Describe the arrangements and procedures that will be used for notifying the licensee who arranges for the physical protection of material in transit of the arrival of the shipment at its destination or of any such shipment that is lost or unaccounted for after the estimated time of arrival at its destination.

9.6 Lost Material Notification [73.67(e)(3)(vi)]

Intent

The intent of this requirement is to ensure that, in the event a shipment becomes overdue and no reasonable explanation has been received from the carrier regarding its status, a trace investigation will be conducted to locate the missing SNM. At this time, the NRC must be notified that the

material is missing and informed as to what steps are being taken to recover the missing material. Although the licensee is responsible for notifying the NRC of any missing material and to initiate and assist in the subsequent investigation, the law enforcement agencies bear the responsibility for physically recovering the material.

Content

Describe what procedures will be used to trace any shipment that is lost or has not arrived by the estimated arrival time. Ensure that all lost or missing material will be immediately reported to the appropriate NRC Regional Office along with what actions are being taken to trace the shipment, that the NRC will be notified as specified in § 73.71, "Reports of Unaccounted-for Shipments, Suspected Theft, Unlawful Diversion, or Industrial Sabotage," and that the shipper or receiver, as appropriate, will also be notified.

10 EXPORT REQUIREMENTS

This chapter provides guidance on meeting the requirements of paragraph 73.67(e)(4), which reads as follows:

(e)(4) Each licensee who exports special nuclear material of moderate strategic significance shall comply with the requirements specified in § 73.67(c), (e)(1) and (e)(3).

Use Chapters 7 and 9 of this part to describe the security procedures that will be used to protect the material up to the point where the receiver accepts physical protection responsibility for the shipment.

11. IMPORT REQUIREMENTS

This chapter provides guidance on meeting the requirements of paragraph 73.67(e)(5), which reads as follows:

(e)(5) Each licensee who imports special nuclear material of moderate strategic significance shall:

(i) Comply with the requirements specified in § 73.67(c), (e)(2) and (e)(3), and

(ii) Notify the exporter who delivered the material to a carrier for transport of the arrival of such material.

11.1 Security Requirements [73.67(e)(5)(i)]

Use Chapters 8 and 9 of Part I of this Standard Format to describe the security procedures that will be used to protect the material from the first point where the shipment is picked up inside the United States.

11.2 Notification [73.67(e)(5)(ii)]

Intent

The intent of this requirement is to ensure that the exporter is notified that the material has arrived safely.

Content

Describe the procedures to be used for notifying the exporter of the material that the shipment has been received.

PART II

SPECIAL NUCLEAR MATERIAL

OF LOW STRATEGIC SIGNIFICANCE

1. USE AND STORAGE AREA AT A FIXED SITE

This chapter provides guidance on meeting the requirement of paragraph 73.67(f)(1), which is as follows:

(f)(1) Store or use such material only within a controlled access area.

A controlled access area (CAA) is defined in paragraph 73.2(z) as "any temporarily or permanently established area which is clearly demarcated, access to which is controlled and which affords isolation of the material or persons within it." "Access control" means measures used to allow only specified personnel, materials, and vehicles ingress into and egress from a given area, while "isolation" refers to measures taken to deter persons, materials, or vehicles from entering or leaving a given area through other than established access control points. Thus, a controlled access area includes provisions for both isolation and access control. In some cases, isolation or access control systems may also serve the purpose of aiding in the detection of unauthorized penetration or activities* within the CAA. Therefore, these detection-related considerations are also alluded to in this chapter.

In the discussion that follows, CAAs intended for the use and possible storage of SNM of low strategic significance are discussed separately from those intended solely for the storage of such SNM. Although there is no difference in the requirements for these two different applications of the CAA, it is recognized that the means used to isolate the material and to control access may differ markedly for use areas compared with storage areas and therefore warrant separate discussion.

1.1 Areas for Use and Temporary Storage [73.67(f)(1)]

This section discusses CAAs intended primarily for the use and temporary storage of SNM of low strategic significance. These may be temporarily established to meet transitory or intermittent SNM use requirements or they may be permanently established. Permanently established CAAs for use of SNM may also be used for storage for short intervals between periods of usage. "Use" means that the material is undergoing processing (e.g. fuel fabrication, irradiation in a reactor, etc.) or utilization of its properties in conjunction with experimental equipment (e.g., research or educational laboratory experiments). Different isolation/access control measures may be used for periods during which the area is occupied versus unoccupied.

a. Temporarily Established CAAs

Temporarily established CAAs for the use of SNM need not have permanent barriers at their boundaries. Isolation of the material and persons using the material may be provided by office partitions, cordons, or other devices used to warn passersby of the restricted nature of the area. Access control can be effected through surveillance or supervision of the area by those who are using the SNM and who are responsible for the material. However,

*Unauthorized activities are those activities deemed by the licensee to be indicative of or contributory to the possible theft of SNM.

the provision of access control through personal supervision is suitable only for those situations in which the size of the CAA and the number of persons to be admitted are sufficiently small and in which the CAA is suitably configured to make such procedures practical.

When material located in a temporarily established CAA is to be left unattended (i.e., because it is impractical to replace the material in a CAA designed for long-term storage of the material), access control and improved isolation for the temporary CAA may be provided to substitute for the discontinued personal supervision over the material. (In addition, provisions must also be made for satisfying the monitoring requirement of paragraph 73.67(f)(2).) Improved isolation can sometimes be provided by increasing the penetration resistance of existing barriers (e.g., locking doors and windows, placing the material in a locked drawer or supply room, etc.). Access control may be provided by any of the measures suggested below for permanently established CAAs left unattended; some of these suggestions may be more suitable for temporary use than others. If no suitable barrier is available to provide isolation, material left unattended can be protected by a motion alarm covering the area immediately surrounding the material. This improved detection capability would be considered an acceptable substitute for the rudimentary isolation provided by temporary barricades, cordons, signs, and other less substantial means of isolation that may be used on a temporary basis.

b. Permanently Established CAAs

Permanently established CAAs for the use and temporary storage of SNM of low strategic significance would most likely provide isolation for the SNM through the use of permanent barriers. These could consist of fences; gates or freestanding walls for exterior areas; or exterior or interior building walls, locked doors, windows, bars, grillwork; or other barriers for interior areas. Such barriers are not required to meet the more stringent criteria for physical barriers used for the protection of formula quantities of strategic special nuclear material (SSNM).* However, good security management practice would dictate that the barrier be substantial enough to deter casual passersby from unauthorized penetration. If the barriers are also designed to aid in detection, the criteria for penetration resistance or tamper-indication in accordance with the specific monitoring procedures to be used also apply.

Access control for permanently established CAAs during periods they are occupied can be provided by personal supervision. However, when these areas are unoccupied or when the size, configuration, or numbers of persons intended to be admitted to the area make personal supervision impractical, other means of access control may be called for. Some of the additional access control measures that may be used for permanently established CAAs in these situations are:

---

*"Strategic special nuclear material" means uranium-235 (contained in uranium enriched to 20 percent or more in the U-235 isotope), uranium-233, or plutonium.

- Stationing of a watchman at CAA access control points,
- Limiting distribution of keys, keycards, or combinations to locks on doors and gates,
- Using a coded badging system to identify authorized personnel at CAA access control points,
- Controlling locked CAA doors and gates by use of remote surveillance (e.g., via intercom or CCTV) by personnel stationed at a centrally located access control facility, or
- Controlling access of personnel, material, and vehicles into CAAs by other means.

It is expected that large facilities (e.g., fuel processing facilities) will have more complex isolation and access control systems than small facilities (e.g., research facilities) in order to achieve comparable levels of protection.

Content

Describe the CAAs where the material will be used. Indicate under what conditions CAAs will be established on a temporary basis. State whether each CAA will also be used for storage. For each CAA identified, provide the following information:

1. A description of the area and its features relative to other facility features, showing the normal routes of ingress to each CAA (including a scale diagram).

2. Descriptions of physical barriers, cordons, walls, partitions, or other means of providing isolation of the CAA, and channelling entry through established access control points into the CAA.

3. The means and criteria used for controlling access into the CAA at established access control points.

4. If more than one CAA is designated, indicate the types of material normally used in each CAA; for temporarily established CAAs, indicate the types of activities normally performed within each area.

1.2 Areas for Permanent Storage [73.67(f)(1)]

Intent

Controlled access areas normally used only for storage of SNM are described in this section. Such CAAs may be very limited in size, since they need only contain the material itself, and access to them is expected to be infrequent. Where small amounts of material are involved, the CAA may consist of relatively small containers such as security cabinets, safes, and locked closets or supply rooms.

Isolation for CAAs intended only for storage usually will be provided by the penetration-resistant features of the perimeter barriers or container walls of the CAA. Such barriers and container walls are not required to meet the more stringent criteria for physical barriers used for the protection of formula quantities of SSNM. However, good security management practice would dictate that the barrier be substantial enough to deter casual passersby from unauthorized penetration. If the barriers are also designed to aid in detection, the criteria for penetration resistance or tamper-indication in accordance with the specific monitoring procedures to be used also apply.

In determining the level of isolation and access control for such CAAs, the minimum time required for extricating SNM from its storage location in relationship to the licensee's time of detection and assessment may need to be taken into account (e.g., fuel assemblies stored in shipping casks or non-selfprotecting fuel residing in non-power reactor cores). The bulkiness, massiveness, and difficulty of movement or disassembly of fresh fuel elements or other forms of low-enriched uranium (LEU) in large quantities such as shipping casks or assemblies may pose sufficient difficulty to persons attempting unauthorized removal within a reasonable time period (relative to CAA monitoring procedures) that they can be considered to provide isolation. Control of access to special equipment and vehicles capable of handling and transporting such items may also be included as integral elements of the access control program for the CAA.

Access control procedures for CAAs designated exclusively for storage are expected to be similar to those described in the previous section for periods when use-type CAAs are unoccupied.

It is expected that large facilities (e.g. fuel processing facilities) will have more complex isolation and access control systems than small facilities (e.g., research reactors) in order to achieve comparable levels of protection.

An illumination level is recommended for the CAA that is sufficiently uniform and bright to detect penetration of or tampering with the CAA containment (in the case of a security cabinet) or unauthorized penetration of or activities within the CAA (in the case of a vault-type room or its equivalent).

Content

(This section needs to be completed only for CAAs designated exclusively for storage of SNM. CAAs designated for both use and storage are to be described as recommended in Section 1.1 of Part II of this Standard Format.)

Describe the CAAs where the material will be stored, if different from those previously described for use. For each such CAA, provide the following information:

1. A description of the area and its features relative to other facility features showing the access control points for the CAA (including a scale diagram).

2. The physical barriers, container walls, or other features that demarcate the perimeter of the CAA and channel entry through only established access control points. If access control is provided by virtue of the bulkiness, massiveness, and difficulty of disassembly of a container or object serving as a CAA, describe the facts relied upon to support such a determination.

3. The means and criteria used for controlling access to the CAA at established access control points.

4. If more than one CAA is designated for the storage of the material, indicate the types of material normally to be stored in each area.

2. DETECTION DEVICES AND PROCEDURES AT A FIXED SITE

This chapter provides guidance for meeting the requirement of paragraph 73.67(f)(2), which is as follows:

(f)(2) Monitor with an intrusion alarm or other device or procedures the controlled access areas to detect unauthorized penetrations or activities.

The purpose of this monitoring activity as stated in paragraph 73.67(a)(2) is to provide "early detection and assessment of unauthorized access or activities by an external adversary within the controlled access area..." and "early detection of removal of special nuclear material by an external adversary from a controlled access area." This should be done to achieve the objective of minimizing the possibilities for unauthorized removal of special nuclear material "consistent with the consequences of such actions," as stated in paragraph 73.67(a) of the effective rule. Thus the earliness of detection afforded by the licensee's physical protection system may vary depending upon the nature and quantity of the material susceptible to unauthorized removal. Further discussion of the earliness of detection required for possible thefts of different types and quantities of special nuclear material of low strategic significance is provided in Section 2.1.

2.1 Earliness of Detection [73.67(a)]

The criteria used for determining the earliness of detection for unauthorized access, activities, or removal of special nuclear material from controlled access areas will depend upon an assessment of the magnitude of the consequences associated with possible misuse of the type and quantity of material that could be removed in a given theft attempt. For special nuclear material of low strategic significance, three distinct cases are considered:

1. Gross theft of low-enriched uranium (LEU)*

2. Minor theft of low-enriched uranium (LEU)

3. Theft of strategic special nuclear material (SSNM) (i.e., SNM of low strategic significance other than LEU.)

Gross theft of LEU refers to the theft of LEU in a sufficiently large quantity that it could yield upon further enrichment or other processing enough material of the type and quantity needed to construct a clandestine fission explosive (CFE) device. This quantity may vary depending on the enrichment and physical and chemical form of the feed material but may roughly be estimated as an amount containing about 75 kilograms of the isotope U-235. Because the most serious consequences to the public health and safety could occur from a theft of this magnitude, a system that would detect a theft sufficiently early to allow for prompt recovery is called for. The NRC believes that, because of the large quantity of material involved and with proper detection systems and procedures, the licensee would be capable of

* Low-enriched uranium is uranium enriched above natural but less than 20% in the U-235 isotope.

detecting a gross theft of LEU between the time of the actual theft and the time it is transported off site.

Minor theft of LEU refers to thefts involving much smaller quantities of LEU such as could be removed by one or two persons in a private vehicle or on one's person. These minor thefts are significant only to the extent that they could be repeated periodically to eventually accumulate an aggregate quantity similar to that which might be obtained in a gross theft. The required degree of earliness of detection of such thefts is related to the time that would be needed by the adversary to obtain a gross amount through repeated thefts. If the amount taken in each of a series of daily thefts is very small, the ultimate time of detection could be as long as six months--the interval between material inventories as required by Part 70. For larger quantities that could be removed in a single theft, but still much less than would constitute a gross theft, it would be reasonable to expect that one in a series of such thefts would be detected before a gross amount could be removed.

Licensees who possess less than gross quantities of LEU need not provide for early detection of a single theft of a gross quantity, but the capability for detecting multiple thefts is as important as it is for those licensees possessing gross quantities.

Thefts from a single facility of SSNM (SNM of low strategic significance other than LEU) are limited by definition to quantities that could not be used to construct a nuclear explosive device; thefts of similar quantities of SSNM from several different facilities could, however, lead to the accumulation of an aggregate quantity that would permit such illicit use. (The consequences of a single theft of such material would have minimal impact on the public health and safety.) Therefore, detection of such thefts is required sufficiently early to ensure early notification to the NRC. The NRC in turn can then notify other licensees of the need to implement appropriate response measures to prevent the accumulation by a single adversary of a formula quantity of material through multiple thefts from different facilities. The NRC believes that there are detection systems and procedures that would allow the licensee to detect a theft of SSNM within approximately two hours.

2.2 Monitoring of Controlled Access Areas [73.67(f)(2)]

Intent

Monitoring of CAAs where the material is used will require a capability for early detection of (a) unauthorized penetration of the CAA perimeter, (b) unauthorized activities within the CAA, (c) unauthorized removal of SNM from the CAA, or (d) some combination of these, by an external adversary. For purposes of this guidance, an external adversary is any person not employed by the licensee or one of his contractors to report for work on a regular basis at the licensee's site and who is not directly involved in the processing or other authorized use of the material in connection with his assigned duties. For purposes of this definition, graduate and other students assigned by the licensee at an educational or research institution to assume responsibility for the regular handling of the material would not be considered an external adversary.

The choice of particular safeguards measures to be included in the CAA monitoring system will depend upon a number of different site specific factors such as whether the measure is to function while the area is occupied or unoccupied, the size of the area, the types of functions performed in the area, the level of traffic into and out of the area, etc. Many of the available safeguards measures which may be employed in the CAA monitoring system are described in various regulatory guides and NUREG series documents issued by the Commission. Specifically, the Fixed Site Physical Protection Upgrade Rule Guidance Compendium* provides guidance on selection, installation, and implementation of monitoring devices and procedures relative to physical protection of formula quantities of SSNM. This guidance is also applicable to monitoring equipment and procedures for CAAs at fixed sites having less than formula quantities of SNM with regard to individual physical protection measures. It is recognized, however, that from a systems point of view, this body of guidance intended to support the Upgrade Rule may emphasize a much greater level of redundancy and diversity than would be required for the protection of SNM of moderate and low strategic significance.** The following paragraphs give illustrations of various monitoring systems that can be used to provide the earliness of detection discussed in Section 2.1.

a. Early Detection of Gross Theft of LEU

Early detection of gross theft of LEU means detection during the attempted theft. This may be accomplished by using intrusion alarms or other monitoring devices in the following applications:

- Fence or buried line perimeter detection systems at the CAA boundaries.
- Door and window alarms (e.g., balanced magnetic switches) for CAAs within buildings and alarms on emergency exit doors equipped with crash bars.
- Volumetric interior motion detection systems for unoccupied CAAs or portions of CAAs within buildings.

In many cases, security procedures may be employed as substitutes for some or all of the devices that could be employed to fulfill the monitoring requirement for the CAA. Security procedures may be especially attractive

---

* The compendium was issued for public comment in conjunction with the proposed Physical Protection Upgrade Rule (42 FR 34310, 7/5/77). It is intended to assist the licensee in the development and implementation of safeguards physical protection and transportation protection plans. Copies are available for inspection at the Commission's Public Document Room, 1717 H Street NW., Washington, D.C.

** Tamper-safing of devices intended for use at facilities having less than formula quantities of strategic special nuclear material need protect only against the external adversary; to the extent such a distinction can be made for a given device, this represents a relaxation in tamper-safing requirements relative to protection of formula quantities.

in protecting against the theft of gross quantities of LEU located outside buildings, where intrusion alarms may more easily be circumvented by an external adversary. Typical security procedures that may be employed for detection of attempts at unauthorized removal of gross quantities of LEU include the following:

- Periodic patrols of CAA perimeters and areas within the CAA by watchmen.
- Surveillance (escorting) of non-licensee vehicles capable of transporting gross quantities of LEU away from the site.
- Continuous (without interruption) or continual (intermittent) surveillance of the CAA, or a given portion of the CAA which contains a gross quantity of LEU, by designated supervisory or other licensee employees. (These surveillance responsibilities could be undertaken in addition to the employee's normal functions provided they can both be discharged adequately.)
- Periodic inspections to confirm continued integrity of barriers, gates, loading bay doors, etc., through which unauthorized removal of gross quantities of LEU could be effected.
- Inspection of large vehicles leaving CAAs to ensure they are not used for unauthorized removal of a gross quantity of LEU.

Where procedures involve periodic patrols or inspections, the amount of time that would be required for an adversary to complete the removal of a gross quantity of LEU may be used to govern the interval between inspections. For example, if a given number of a certain type of container of LEU would have to be individually loaded onto a truck in order to effect removal of a gross quantity of LEU and the time required for such loading is determined to be in excess of two hours, then a two-hour guard patrol of the given area would be considered to meet the earliness-of-detection guideline for the subject material.

A combination of these and perhaps other measures could satisfy the early detection criterion for gross theft of LEU if it could be shown that an external adversary could not obtain unauthorized access to the SNM without being detected by at least one intrusion alarm component.

b. Early Detection of Minor Theft of LEU

The criteria for early detection of minor theft of LEU can be satisfied by a monitoring program that provides a sufficiently high probability of detection of one in a series of minor thefts so it is implausible that an adversary would be able to obtain in the aggregate a gross quantity of LEU. Such a capability could be provided in whole, or in part, by the same monitoring program designed to detect gross theft. Additional measures that might be included in the monitoring program to protect against minor theft include the following:

Exit searches of non-licensee vehicles capable of transporting hand-carried quantities of LEU (on random or general basis).

- Administrative control of materials removed from controlled areas where easily concealed or hand-carried items containing LEU are available.

- Item count inventories more frequent than those currently required under Part 70.

- Procedures directing regular employees to be aware of unauthorized persons in their work areas and to report the presence of such persons to supervisory or security personnel. (A coded badging program would support this measure.)

- Escorting of visitors and other unauthorized persons entering CAA.

- Watchman patrols to detect unauthorized persons within the CAA.

- SNM doorway monitors at all personnel access control points.

These are not required measures, but illustrations of how the monitoring program for detecting gross theft of LEU may be extended to include the capability for early detection of minor theft of LEU. One or more of these measures may be employed, but probably not all of them would be needed for any one installation.

c. Early Detection of Theft of SSNM (SNM of low strategic significance other than LEU)

For facilities where it is necessary to protect against thefts of SNM of low strategic significance other than LEU (SSNM), earliness of detection is discussed in Section 2.1 of this chapter. The physical protection system in this case may differ considerably from that designed to protect LEU. The sites are likely to be small research-oriented facilities such as non-power reactors and educational institutions. Also, there is likely to be much less material available, and authorized access to it may be less frequent. Detection devices such as interior motion detector systems, balanced magnetic switches, etc. could be used to monitor relatively small CAAs where the number of established access control points is very limited.

Procedures may also be used to protect against thefts of SSNM in this subcategory. Since watchman patrols inherently allow unguarded intervals during which an external adversary could conceivably obtain access to the CAA, remove a small amount of material, and leave before being discovered, the inspection procedure may (a) be sufficiently frequent to ensure an external adversary could not complete a successful theft of the material during the unguarded intervals, (b) provide for an irrevocable indication of the CAA barrier having been tampered with (as with a seal or by observation of damage done to the barrier), or (c) provide for an item count inventory or other accounting for the material as part of the inspection. Some examples are given below:

- After having left material unattended in an experimental setup in a classroom used as a temporary CAA, the instructor returns after two hours and verifies that the material is still in place.

- A small quantity of material is stored in a security cabinet for several months at a time without authorized access. Every two hours a watchman comes around to inspect the cabinet to ensure that the lock is secure and the cabinet has not been tampered with. If a suitable combination or other pick-resistant lock is not used, the watchman also inspects a tamper-indicating seal to verify that the container has not been tampered with.

- During times when a non-power reactor is left unattended, a watchman comes around every two hours and checks that none of the fuel elements have been removed by unauthorized persons. If he encounters a person working during off-hours in the vicinity of the reactor, he asks for appropriate identification.

- While a non-power reactor is being utilized, the supervisor ensures that he or his designee is not away from the reactor for a period longer than thirty minutes, a period he estimates would be minimally required for a person to secure fuel elements in the core that were not self-protecting by virtue of their having been sufficiently irradiated.

- During periods when excess fuel is left unattended in a storage closet at a non-power reactor facility, an alarm system is activated that would annunciate if anybody tried to penetrate the closet without proper authorization.

During periods when the material is being used under the direct supervision of authorized personnel, the monitoring requirement is satisfied by virtue of the continuous surveillance by the authorized personnel.

Content

For each of the CAAs described previously (see Part II, Chapter 1, of this guide), provide the following information regarding the measures taken to fulfill the monitoring requirement of paragraph 73.67(f)(2):

1. Describe any devices employed by specifying the type of device, its installed location, the type and location of annunciation, its intended area of coverage, and its tamper-resistant features. Refer, if desired, to existing filed security plans or NRC-published guidance or NUREG series documents.

2. Describe any procedures employed to monitor the CAA or portions thereof, including the categories of persons who will execute the procedures, the frequency of inspections or rounds of patrol, the basis for the determination of such frequencies, and the occasions upon which the procedures are intended to be implemented. Indicate, also, the features of the CAA (e.g. barriers, locks, seals, etc.) that will play a role in the way the procedures are used.

3. Explain how the combination of procedures and devices used to monitor each CAA meets the criteria for early detection of theft by an external adversary relative to the type of material found in each CAA.

3. SECURITY RESPONSE AT A FIXED SITE

This chapter provides guidance on meeting the requirement of paragraph 73.67(f)(3), which is as follows:

(f)(3) Assure that a watchman or offsite response force will respond to all unauthorized penetrations or activities.

Intent

The intent of this requirement is to ensure that, in the event of a security incident, someone will be available to assess alarms or any unauthorized penetrations or activities and, if warranted, notify the NRC, the local law enforcement authorities, and the responsible person in licensee management. Early detection and notification of any missing material will help facilitate its prompt recovery. For the purpose of this regulation, an offsite response force can be a local law enforcement agency or a contract guard service.

Content

Describe the security organization that will be responsible for assessing and responding to any unauthorized penetrations or activities. Ensure that at least one guard, watchman, or member of an offsite response force will respond to all unauthorized penetrations or security incidents at the CAAs.

4. RESPONSE PROCEDURES AT A FIXED SITE

This chapter provides guidance on meeting the requirements of paragraph 70.67(f)(4), which states:

(f)(4) Establish and maintain response procedures for dealing with threats of thefts or thefts of such material.

Intent

The intent of this regulation is to help the licensee to identify those security incidents that could result in the loss of SNM of low strategic significance and to develop response procedures to prevent or reduce the likelihood of such a loss. Some types of incidents that should be considered and for which response procedures should be developed are:

1. Situations that could possibly lead to theft of SNM (e.g. civil disturbance).

2. Discovery that the security system has been breached.

3. Discovery that some SNM is missing.

Content

Identify those events for which response procedures will be developed. Also describe the type of response to be accomplished for each event identified and the duties and responsibilities of the security organization and management involved in the response. Ensure that the NRC will be notified immediately in the event of theft or attempted theft of the material. Describe what local law enforcement assistance is available, their response capabilities, and any agreements made with them to respond in the case of theft of the material.

5. MATERIAL TRANSPORTATION REQUIREMENTS

This chapter provides guidance on meeting the requirements of paragraph 73.67(g)(1), which are as follows:

(g)(1) Each licensee who transports or who delivers to a carrier for transport special nuclear material of low strategic significance shall:

(i) Provide advance notification to the receiver of any planned shipments specifying the mode of transport, estimated time of arrival, location of the nuclear material transfer point, name of carrier and transport identification,

(ii) Receive confirmation from the receiver prior to commencement of the planned shipment that the receiver will be ready to accept the shipment at the planned time and location and acknowledges the specified mode of transport,

(iii) Transport the material in a tamper-indicating sealed container,

(iv) Check the integrity of the containers and seals prior to shipment, and

(v) Arrange for the in-transit physical protection of the material in accordance with the requirements of §73.67(g)(3) of this part, unless the receiver is a licensee and has agreed in writing to arrange for the in-transit physical protection.

5.1 Advance Notification [73.67(g)(1)(i)]

Intent

The intent of this paragraph is to require the shipper to preplan the transportation of the material and inform the receiver of his plans prior to shipment. This is the first of several transportation requirements that will allow the receiver to take delivery of the material as planned or to help ensure traceability of any missing material.

Content

The licensee should ensure that, prior to each shipment of material, the receiver will be notified of the impending shipment and provided the following types of information:

1. Mode of transport (e.g., truck, plane, train, or ship),

2. Estimated time of arrival,

3. Location where material is to be transferred to receiver,

4. Name of carrier, and

5. Transport identification (e.g., truck, train, or flight number; ship name).

5.2 Receiver Confirmation [73.67(g)(1)(ii)]

Intent

The intent of this requirement is that, prior to shipment, the transporter will be assured that the receiver is ready to accept the shipment at the planned time and location and has acknowledged the mode of transport.

Content

Describe what procedures will be used to ensure that shipment of material does not take place until the receiver acknowledges the planned shipment and mode of transport and states that he will be ready to accept the shipment at the planned time and location.

5.3 Container [73.67(g)(1)(iii)]

Intent

The intent of this requirement is to provide a mechanism or system that will help the receiver detect any tampering with the material's container that may have occurred during shipment. Regulatory Guide 5.15, "Security Seals for the Protection and Control of Special Nuclear Material," provides guidance in this area. If the material is shipped in an exclusive-use carrier, it is acceptable to tamper-seal the carrier itself rather than each individual SNM container.

Content

Describe the types of seals that will be used to secure the material's container during transport.

5.4 Inspection [73.67(g)(1)(iv)]

Intent

The intent of this paragraph is to require the shipper to check the integrity of the material container's seals just prior to shipment so that he can be assured that they have not been compromised. Then, upon receipt of the shipment, if the receiver discovers the container's integrity has been compromised and the material is missing, the scope of the recovery operation can focus on the transportation route.

Content

Describe the procedures to be used to ensure that the integrity of the containers or seals is checked just prior to shipment.

5.5 Responsibility for In-Transit Physical Protection [73.67(g)(1)(v)]

Intent

The intent of this paragraph is to make clear that the licensee shipping the material is responsible for arranging for the physical protection of the material in transit if the receiver is not a licensee. If both the shipper and receiver are licensees, the shipper may allow the receiver to accept this responsibility wholly or in part provided there is appropriate documentation specifying their respective responsibilities. Where no such documentation exists, both the shipper and receiver are held jointly responsible. (See Section 6.3 in the next chapter.)

Content

In his security plan, the shipper should either acknowledge responsibility for the in-transit physical protection of SNM of low strategic significance or ensure that a written agreement from the receiver has been received in which the receiver accepts either full responsibility or shared responsibility for the in-transit physical protection of this material in accordance with paragraph 73.67(g)(3) of 10 CFR Part 73.

6. RECEIVER REQUIREMENTS--TRANSPORTATION

This chapter provides guidance on meeting the requirements of paragraph 73.67(g)(2), which are as follows:

(g)(2) Each licensee who receives quantities and types of special nuclear material of low strategic significance shall:

(i) Check the integrity of the containers and seals upon receipt of the shipment,

(ii) Notify the shipper of receipt of the material as required in §70.54 of Part 70 of this chapter, and

(iii) Arrange for the in-transit physical protection of the material in accordance with the requirements of paragraph 73.67(g)(3) of this part, unless the shipper is a licensee and has agreed in writing to arrange for the in-transit physical protection.

6.1 Inspection [73.67(g)(2)(i)]

Intent

This requirement is intended to determine whether the material's container has been compromised enroute and whether any material has been removed so that immediate recovery procedures can be initiated if required.

Content

Describe the procedures to be used to ensure that the integrity of the containers and seals will be checked upon receipt of the material shipment.

6.2 Notification [73.67(g)(2)(ii)]

This requirement is intended to:

1. Ensure that knowledge of the current location of all SNM is available, and

2. Formally inform the shipper that the material has been received.

Content

Ensure that a completed copy of Form NRC-741, "Nuclear Material Transaction Report," will be sent to the shipper within 10 days after a material shipment has been received as required in §70.54 of 10 CFR Part 70.

6.3 Responsibility for In-Transit Physical Protection [73.67(g)(2)(iii)]

Intent

The intent of this paragraph is to make clear that the licensee receiving the material is responsible for arranging for the physical protection of the material in transit if the shipper is not a licensee. If both the shipper

and receiver are licensees, the receiver may allow the shipper to accept this responsibility either wholly or in part provided there is appropriate documentation specifying their respective responsibilities. Where no such documentation exists, both the shipper and receiver are held jointly responsible. (See Section 5.5 in the preceding chapter).

Content

In his security plan, the receiver should either acknowledge responsibility for the in-transit physical protection of SNM of low strategic significance or ensure that a written agreement from the shipper has been received in which the shipper accepts either full responsibility or shared responsibility for the in-transit physical protection of this material in accordance with paragraph 73.67(g)(3) of 10 CFR Part 73.

7. IN-TRANSIT PHYSICAL PROTECTION REQUIREMENTS

This chapter provides guidance on meeting the requirements of paragraph 73.67(g)(3), which are as follows:

(g)(3) Each licensee, either shipper or receiver, who arranges for the physical protection of special nuclear material of low strategic significance while in transit or who takes delivery of such material free on board (f.o.b.) the point at which it is delivered to a carrier for transport shall:

(i) Establish and maintain response procedures for dealing with threats of thefts or thefts of such material,

(ii) Make arrangements to be notified immediately of the arrival of the shipment at its destination, or of any such shipment that is lost or unaccounted for after the estimated time of arrival at its destination, and

(iii) Conduct immediately a trace investigation of any shipment that is lost or unaccounted for after the estimated arrival time and report to the Nuclear Regulatory Commission as specified in §73.71 and to the shipper or receiver as appropriate. The licensee who made the physical protection arrangements shall also immediately notify the Director of the appropriate Nuclear Regulatory Commission Inspection and Enforcement Regional Office listed in Appendix A of the action being taken to trace the shipment.

7.1 Response Procedures [73.67(g)(3)(i)]

Intent

The intent of this regulation is to help the licensee identify those transportation incidents that could affect the security of the SNM in transit for which he might expect to be notified and for which response procedures should be planned.

Content

Identify those events for which response procedures will be developed. Also describe the type of response to be accomplished for each event identified and the duties and responsibilities of the security organization and management involved in the response. Ensure that the NRC will be notified immediately in the event of theft or attempted theft of the material.

7.2 Notification [73.67(g)(3)(ii)]

Intent

The intent of this requirement is to ensure that the licensee responsible for the physical protection of SNM in transit will have a firm basis for deciding whether or not to initiate response procedures in the event a shipment becomes overdue or is lost.

Content

Describe the arrangements and procedures that will be used for notifying the licensee who arranges for the physical protection of material in transit (1) of the arrival of the shipment at its destination or (2) of any such shipment that is lost or unaccounted for after the estimated time of arrival at its destination.

7.3 Lost Material Notification [73.67(g)(3)(iii)]

The intent of this requirement is to ensure that, in the event a shipment becomes overdue and no reasonable explanation has been received from the carrier regarding its status, a trace investigation will be conducted to locate the missing SNM. At this time, the NRC should be notified that the material is missing and informed as to what steps are being taken to recover it. Although the licensee is responsible for notifying the NRC of any missing material and for initiating and assisting in the subsequent investigation, the law enforcement agencies bear the responsibility for physically recovering the material.

Content

Describe what procedures will be used to trace any shipment that is lost or has not arrived by the estimated arrival time. Ensure that all lost or missing material will be immediately reported to the appropriate NRC Regional Office along with what actions are being taken to trace the shipment, that the NRC will be notified as specified in §73.71, and that the shipper or receiver, as appropriate, will also be notified.

8. EXPORT REQUIREMENTS

This chapter provides guidance on meeting the requirements of paragraph 73.67(g)(4), which reads as follows:

(g)(4) Each licensee who exports special nuclear material of low strategic significance shall comply with the appropriate requirements specified in §73.67(c), (g)(1) and (g)(3).

Use Chapters 5 and 7 of Part II of this Standard Format to describe the security procedures that will be used to protect the material up to the point where the receiver accepts physical protection responsibility for the shipment.

9. IMPORT REQUIREMENTS

This chapter provides guidance on meeting the requirements of paragraph 73.67(g)(5), which reads as follows:

(g)(5) Each licensee who imports special nuclear material of low strategic significance shall:

(i) Comply with the requirements specified in §73.67(c), (g)(2) and (g)(3), and

(ii) Notify the person who delivered the material to a carrier for transport of the arrival of such material.

9.1 Security Requirements [73.67(g)(5)(i)]

Use Chapters 6 and 7 of Part II of this Standard Format to describe the security procedures that will be used to protect the material from the first point where the shipment is picked up.

9.2 Notification [73.67(g)(5)(ii)]

Intent

The intent of this regulation is to ensure that the exporter is notified that the material has arrived safely.

Content

Describe the procedures to be used for notifying the exporter of the material that the shipment was received.

VALUE/IMPACT ASSESSMENT

A separate value/impact analysis has not been prepared for this regulatory guide. The guide was developed to provide a standard format and content for the physical protection plans that licensees authorized to possess or transport special nuclear material of moderate strategic significance or 10 kilograms or more of material of low strategic significance are required to submit by amendments to Part 73 of the Commission's regulations published July 24, 1979 (44 FR 43280). A value/impact analysis prepared for the amendments was made available in the Commission's Public Document Room at the time the amendments were published. This analysis is also appropriate to this regulatory guide.

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

OFFICIAL BUSINESS
PENALTY FOR PRIVATE USE, $300

POSTAGE AND FEES PAID
U.S. NUCLEAR REGULATORY
COMMISSION

U.S. MAIL

[redacted]19406002001 1 D5DAQ5QA
US NRC REGION I
OFFICE OF INSPECTION & ENFORCE
J BORES
631 PARK AVENUE
REGION I
KING OF PRUSSIA PA 19406