



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

July 10, 1980

Regulatory Guide 5.52  
Revision 2

REGULATORY GUIDE DISTRIBUTION LIST (DIVISION 5)

SUBJECT: Regulatory Guide 5.52, Revision 2, "Standard Format and Content of a Licensee Physical Protection Plan for Strategic Special Nuclear Material at Fixed Sites (Other than Nuclear Power Plants)"

Regulatory Guide 5.52, Revision 2, was distributed for comment to all affected licensees and to other interested parties who attended the NRC Upgrade Rule Guidance Seminar held on March 27-28, 1979, in Richmond, Virginia. No comments were received as a result of this distribution, and Revision 2 of the guide is now being issued as an active guide so that affected licensees may use it for preparation of their physical protection plans in response to the new requirements of 10 CFR Part 73 published in the Federal Register on November 28, 1979 (44 FR 68184).

Among other changes, the transportation material has been removed from Revision 2 of Regulatory Guide 5.52 and is now found in Regulatory Guide 5.60, "Standard Format and Content of a Licensee Physical Protection Plan for Strategic Nuclear Material in Transit."

Because Regulatory Guide 5.52, Revision 2, was not issued as a proposed revision for comment, it is being provided as an active guide to all addressees on the Division 5 distribution list. Although comments are always encouraged on all regulatory guides, comments on this guide are particularly encouraged at this time.

Robert B. Minogue, Director  
Office of Standards Development



U.S. NUCLEAR REGULATORY COMMISSION

Revision 2\*  
July 1980

# REGULATORY GUIDE

OFFICE OF STANDARDS DEVELOPMENT

## REGULATORY GUIDE 5.52

### STANDARD FORMAT AND CONTENT OF A LICENSEE PHYSICAL PROTECTION PLAN FOR STRATEGIC SPECIAL NUCLEAR MATERIAL AT FIXED SITES (OTHER THAN NUCLEAR POWER PLANTS)

\*The transportation material has been removed from this guide and is now found in Regulatory Guide 5.60, "Standard Format and Content of a Licensee Physical Protection Plan for Strategic Special Nuclear Material in Transit." The substantial number of additional changes has made it impractical to indicate the changes with lines in the margin.

#### 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

	<u>Page</u>
INTRODUCTION.....	vii
 <b>PART I - <u>GENERAL ISSUES</u></b>	
1. OVERVIEW OF SITE AND FACILITY.....	3
2. THREATS.....	3
3. LOCAL LAW ENFORCEMENT AGENCY COMMITMENTS.....	3
3.1 Size of Force.....	3
3.2 Kind of Assistance.....	3
4. CONTINGENCY PLAN.....	4
5. GUARD FORCE QUALIFICATION AND TRAINING.....	4
6. SECURITY MANAGEMENT.....	4
7. QUALITY ASSURANCE PROGRAMS.....	4
8. TESTING AND INSPECTION.....	4
8.1 Tests and Inspections During Installation.....	4
8.2 Preoperational Tests and Inspections.....	5
8.3 Operational Tests and Inspections.....	5
9. MAINTENANCE PROGRAMS.....	5
10. SECURITY AUDITS.....	5
10.1 Program Audits.....	5
10.2 Compliance Audits.....	5
11. SECURITY RECORDS.....	5
11.1 Security Tours, Inspections, and Tests.....	6
11.2 Maintenance.....	6
11.3 Alarm Annunciations.....	6
11.4 Security Response.....	6
11.5 Authorized Individuals.....	6
11.6 Nonemployee Access.....	6
12. REPORTS TO NRC.....	6
12.1 Incidents.....	6
12.2 Unusual Occurrences.....	6
12.3 Protection Plan Changes.....	7
13. SCHEDULE FOR IMPLEMENTATION.....	7
14. REDUNDANCY AND DIVERSITY.....	7
15. PHYSICAL PROTECTION SYSTEM INTEGRITY.....	7
16. PHYSICAL PROTECTION SYSTEM POWER SOURCES.....	7

TABLE OF CONTENTS (Continued)

	<u>Page</u>
17. ALARM STATIONS.....	7
17.1 Central Alarm Station.....	8
17.2 Secondary Alarm Station.....	8
 <u>PART II - SPECIFIC SYSTEM PERFORMANCE</u>	
18. PREVENT UNAUTHORIZED ACCESS OF PERSONS AND MATERIALS INTO MATERIAL ACCESS AREAS AND VITAL AREAS.....	12
18.1 Entry Control Through MAA and VA Entry Portals.....	12
18.1.1 Entry Authorization Procedures.....	12
18.1.2 Entry Procedures and Controls for Routine Conditions.....	12
18.1.3 Entry Procedures and Controls for Nonroutine Conditions.....	13
18.1.4 Bypass of Admittance Procedures and Controls.....	13
18.2 Entry Through Remainder of the MAA/VA Boundary.....	14
18.2.1 Detect Boundary Penetration Attempt.....	14
18.2.2 Deter Boundary Penetration Attempt.....	14
18.2.3 Respond to Boundary Penetration Attempt.....	14
19. PERMIT ONLY AUTHORIZED ACTIVITIES AND CONDITIONS WITHIN PROTECTED AREAS, MATERIAL ACCESS AREAS, AND VITAL AREAS.....	14
19.1 Permit Only Authorized Activities and Conditions Within Protected Area.....	14
19.1.1 Establishment of Authorized Activities and Conditions.....	14
19.1.2 Prevention of Unauthorized Activities and Conditions.....	15
19.2 Permit Only Authorized Activities and Conditions Within MAA..	15
19.2.1 Establishment of Authorized Activities and Conditions.....	15
19.2.2 Prevention of Unauthorized Activities and Conditions.....	15
19.3 Permit Only Authorized Activities and Conditions Within VA...	15
19.3.1 Establishment of Authorized Activities and Conditions.....	15
19.3.2 Prevention of Unauthorized Activities and Conditions.....	15

TABLE OF CONTENTS (Continued)

	<u>Page</u>
20. PERMIT ONLY AUTHORIZED PLACEMENT AND MOVEMENT OF SSNM WITHIN MAAs.	15
20.1 Establishment of Authorized Placement and Movement of SSNM...	15
20.2 Establishment of Current Knowledge of SSNM.....	16
20.3 Prevention of Unauthorized Placement and Movement of SSNM....	16
21. PERMIT REMOVAL OF ONLY AUTHORIZED AND CONFIRMED FORMS AND AMOUNTS OF SSNM FROM MAAs.....	16
21.1 Control of SSNM Removal Through MAA Portals.....	16
21.1.1 Development of Removal Authorization Procedures.....	16
21.1.2 Removal Procedures and Controls for Normal Conditions.....	16
21.1.3 Removal Procedures and Controls Under Emergency Conditions.....	17
21.1.4 Bypass of Removal Procedures.....	18
21.2 Removal of SSNM Through Remainder of Boundary.....	18
22. PROVIDE FOR AUTHORIZED ACCESS AND ASSURE DETECTION OF AND RESPONSE TO UNAUTHORIZED PENETRATIONS OF PA.....	18
22.1 Entry Control Through PA Entry Portals.....	18
22.1.1 Entry Authorization Procedures.....	18
22.1.2 Entry Procedures and Controls for Normal Conditions..	18
22.1.3 Procedures and Controls for Emergency Entry of Personnel and Vehicles.....	19
22.1.4 Prevention of Bypass of Entry Procedures and Controls.....	19
22.2 Entry Through Remainder of PA Boundary.....	20
23. RESPONSE.....	20
23.1 Communications.....	20
23.1.1 Communications with Onsite Forces.....	20
23.1.2 Communications with Offsite Forces.....	20
23.2 Effective Response.....	21
23.2.1 Onsite Response.....	21
23.2.2 Offsite Response.....	21

TABLE OF CONTENTS (Continued)

	<u>Page</u>
<u>APPENDIX 1 - COMPONENTS AND MEASURES LIST AND INFORMATION REQUEST SHEETS</u>	
A. Physical Protection Components and Measures List.....	23
B. Physical Protection Components and Measures Information Request Sheets.....	27
<u>ATTACHMENT A - SAMPLE PORTION OF PHYSICAL PROTECTION PLAN.....</u>	73

## INTRODUCTION

The Atomic Energy Act of 1954, as amended, directed the 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 for physical protection of licensed activities against theft and radiological sabotage of strategic special nuclear material (SSNM) at fixed sites are found in 10 CFR Part 50, "Domestic Licensing of Production and Utilization Facilities," Part 70, "Domestic Licensing of Special Nuclear Material," and Part 73, "Physical Protection of Plants and Materials."

Paragraph 50.34(c) of 10 CFR Part 50 and paragraphs 70.22(g) and 70.22(h) of 10 CFR Part 70 identify the physical protection information that must be provided in a Physical Protection Plan as part of a license application in order for the applicant to demonstrate compliance with the specific physical protection requirements of 10 CFR Part 73. A Physical Protection Plan must be submitted with each application for a license to possess SSNM.

On August 23, 1978, the NRC published Appendix B, "General Criteria for Security Personnel," to 10 CFR Part 73, which became effective on October 23, 1978. These criteria prescribe upgraded qualifications and training requirements for security personnel, including upgraded equipment requirements for armed personnel responding to threats at certain fixed site nuclear facilities.

On November 28, 1979, the NRC published amendments (known as the Physical Protection Upgrade Rule) to 10 CFR Part 73. These amendments prescribed general performance objective requirements as well as performance capabilities necessary to protect against prescribed adversaries. The general performance requirements are the same for both fixed sites and for transportation activities. The performance capabilities describe the functions to be performed by a licensee's physical protection program. Performance capabilities differ for fixed sites and for transportation, reflecting the basic differences inherent in fixed site protection as opposed to the protection of moving vehicles and transfer point installations.

Although primarily designed to prevent theft, the new physical protection requirements also provide increased protection against sabotage.

All the fixed site physical protection requirements contained in the current regulation (§§ 73.1, 73.20, 73.45, and 73.46) are addressed herein.

### Purpose and Applicability

This regulatory guide describes the standard format and content suggested by the NRC for use in preparing fixed site Physical Protection Plans in response to the Physical Protection Upgrade Rule (portions of 10 CFR Part 73). By using this Standard Format for preparing a Physical Protection Plan, the license applicant will minimize administrative problems associated with the submittal, review,

and approval of the plan. Preparation of a Physical Protection Plan in accordance with this Standard Format will assist the NRC in evaluating the plan and in standardizing the licensing and review process. Conformance with this guide is not required by the NRC. An applicant who uses a format that will provide an equal level of completeness and detail may use his own format. The Standard Format does, however, represent a format acceptable to the NRC staff.

Any license application that is required by paragraph 70.21(f) to be filed at least 9 months before construction begins should include the information requested in Chapters 1 through 8 and 13 through 17 of this Standard Format. That information should be designated as the design objective Physical Protection Plan. This design information is needed early in the licensing process to ensure that plant features needed to meet materials and plant protection requirements are included in the facility design.

This Standard Format is applicable to fuel reprocessing plants, fuel manufacturing plants, and other fixed site special nuclear material operations involving the possession or use of uranium-235 (contained in uranium enriched to 20 percent or more in the U-235 isotope), uranium-233, or plutonium alone or in any combination in a quantity of 5000 grams or more computed by the formula:  $\text{grams} = (\text{grams contained U-235}) + 2.5 (\text{grams U-233} + \text{grams plutonium})$ . This document is not intended to be used for nuclear power plant licensees or Category II/III licensees.

The major regulatory sections addressed by Physical Protection Plans written in accordance with this guide are §§ 73.1, 73.20, 73.45, and 73.46. References are made herein to other regulatory sections as appropriate.

The information requested in this Standard Format is typical of that needed for a license application. Additional information may be required for completion of the staff review of a particular application. The applicant should include additional information 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.

Information and procedures delineated in regulatory guides in Division 5, "Materials and Plant Protection," and appropriate to certain sections of the Physical Protection Plan may be incorporated by reference.

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

### Organization and Use of This Document

This guide is divided into three major parts, as the licensee Physical Protection Plan should be. In addition, this guide includes a sample portion of a hypothetical protection plan. Each of the three portions and the sample protection plan are discussed below.

Part I of the Standard Format is divided into 17 chapters that will provide the NRC with an overview of the subject facility and its proposed physical protection program. Certain major aspects of the security system itself such as the

Central Alarm Station (CAS) and the Secondary Alarm Station (SAS) are also addressed in Part I.

Part II of this guide is divided into six chapters that parallel the Performance Capability of the Upgrade Rule (§ 73.45). Each chapter of Part II is broken into sections that address functions required to accomplish each Performance Capability. The applicant is asked to identify each component or measure to be used to accomplish the various parts of each capability and to describe how those components fit into an overall physical protection system. For guidance on potential ways to meet the Performance Capabilities, a "reference system" (§ 73.46) is provided. A chart relating the Performance Capabilities to the reference system is contained in Regulatory Guide 5.61, "Intent and Scope of the Physical Protection Upgrade Rule Requirements for Fixed Sites."

The third major part of this guide (Appendix 1) is composed of a Physical Protection Components and Measures List and a set of Physical Protection Components and Measures Information Request Sheets. The Components and Measures List enumerates typical physical protection measures that could be used in a complete protection system. For each component or measure on the list, a unique Information Request Sheet is provided that outlines the data that the applicant should provide in Appendix 1 to his plan if he has elected to use that particular component.

A diagrammatic representation of how the protection plan should be organized is given in Figure 1.

#### Sample Portion of Protection Plan

As an aid in the preparation of Part II of the Physical Protection Plan and of responses to the Information Request Sheets of Appendix 1, a sample portion of a protection plan for a hypothetical facility is provided as Attachment A. This sample will help in understanding the level of detail needed by the NRC in the licensing and inspection processes and the ways in which to format the information.

#### Protection Plan Format

The applicant should follow the numbering system of this Standard Format. Under some circumstances, certain subsections 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 information in support of his application 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 Appendix 2 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.

# ORGANIZATION OF THE PHYSICAL PROTECTION PLAN

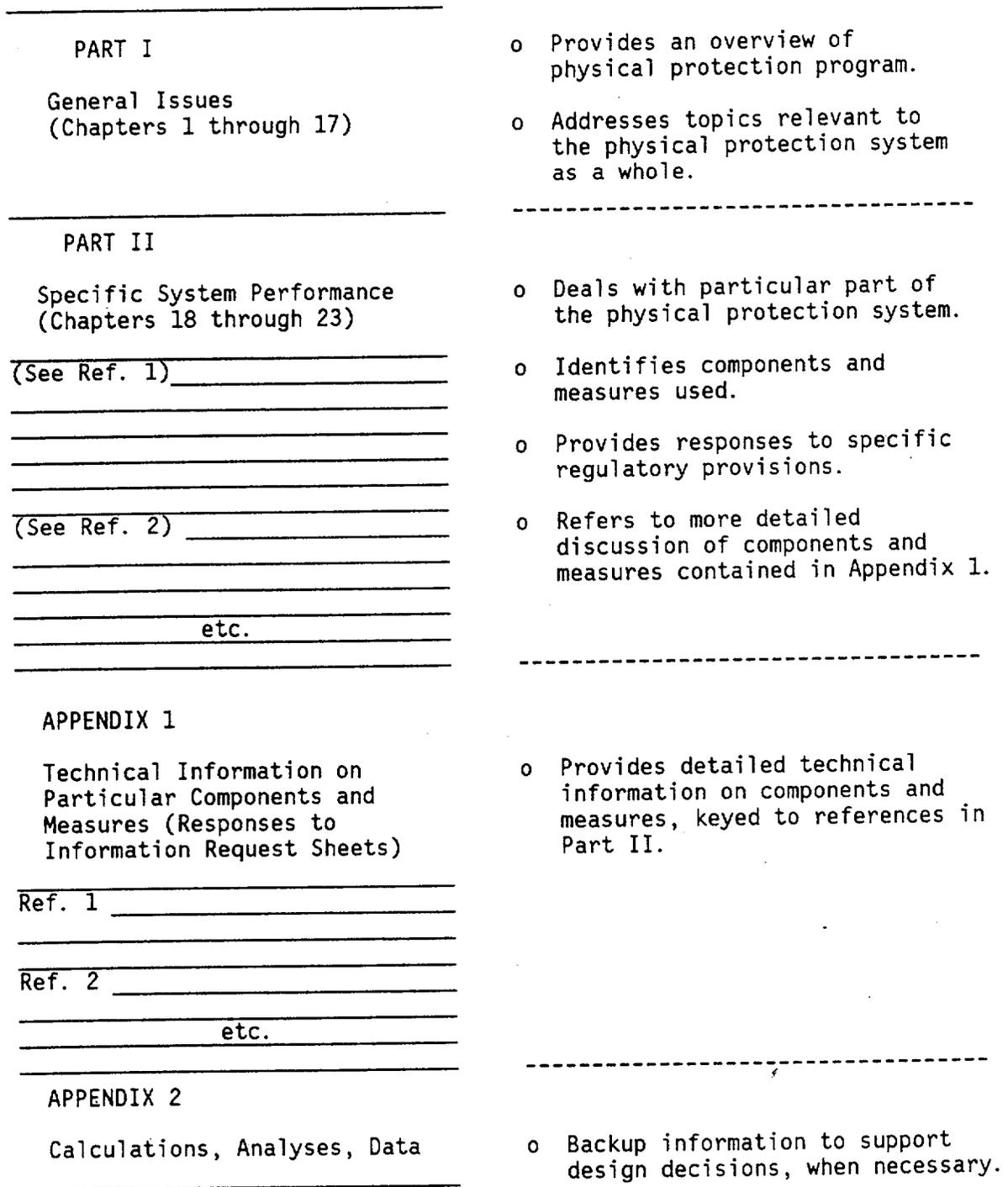


FIGURE 1

## 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 application 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 1 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.)

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. The line should be on the margin opposite the binding margin for each line changed or added. All pages submitted to update, revise, or add pages to the report are to 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 in accordance with paragraph 50.30(c) of 10 CFR Part 50 and § 70.21 of 10 CFR Part 70.

Public Disclosure

The NRC has determined that public disclosure of the details of physical protection programs is not in the public interest, and such details are withheld in accordance with 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 submittal of proprietary information should request exemption from public disclosure, as required in paragraph 2.790(b) of 10 CFR Part 2.

Compatibility

The applicant should ensure that the Physical Protection Plan is compatible with the other sections of his application.

Schedule for Submittal

The applicant should submit his plan in accordance with the schedule provided in paragraph 73.20(c).

**PART I**  
**GENERAL ISSUES**

In Part I of the Physical Protection Plan, the applicant should provide general discussions on the topics of Chapters 1 through 17. Before preparing Part I, the applicant should thoroughly review the entire Standard Format, including Part II and Appendix 1. This review will aid in establishing an appropriate level of detail to be included in each part of the plan. As previously indicated, the discussions in Part I should provide necessary overview information. Increasingly detailed discussions of system specifics and component and measure specifications should be addressed in Part II and Appendix 1, respectively.

## 1. OVERVIEW OF SITE AND FACILITY

Describe the general layout of the facility and the surrounding site. Include a map of the entire facility and other maps and illustrations as appropriate. Indicate on these maps the locations of physical protection systems, subsystems, and major components; also indicate the location of all material access areas, vital areas, vaults, entry/exit control points, and alarm stations. Describe the relationship between physical protection and other activities at the facility.

## 2. THREATS

Affirm the intent to prevent, with high assurance, the theft of special nuclear material (SNM) and to protect against radiological sabotage by the threat defined in § 73.1. For each of the design basis threats specified in § 73.1, describe and evaluate the relationship of the design basis threat to the facility and its operations.

## 3. LOCAL LAW ENFORCEMENT AGENCY COMMITMENTS

Describe the agreements between local law enforcement agencies (LLEAs) and the facility security management regarding response and support during contingency events; also describe the liaisons established between the facility security management and the LLEAs, specifying the officials who perform this function, the frequency of communication, and the nature of these communications. This chapter should include a map showing the location of LLEA facilities in relationship to the licensee's facility and the routes that LLEA personnel might use in responding to an alarm.

### 3.1 Size of Force

Discuss the number and composition of law enforcement personnel available for assistance and the estimated response time for such personnel to reach the facility. Include in the discussion the number of armed individuals in each complement and the time required for each complement to arrive if the complements are to arrive at intervals.

### 3.2 Kind of Assistance

Identify the type or kind of assistance such as police power, investigative work, crowd control, or bomb searches that can be provided and the kind of equipment available.

#### 4. CONTINGENCY PLAN

Briefly describe the facility Contingency Plan prepared in accordance with Appendix C, "Licensee Safeguards Contingency Plans," to 10 CFR Part 73. Relate the Contingency Plan to this Physical Protection Plan.

#### 5. GUARD FORCE QUALIFICATION AND TRAINING

Affirm that an approved Guard Force Training Plan in accordance with Appendix B, "General Criteria for Security Personnel," to Part 73 is in effect. Briefly relate the Guard Force Training Plan to this Physical Protection Plan.

#### 6. SECURITY MANAGEMENT

Describe the structure and management of the security organization, including both uniformed security personnel and other persons responsible for security-related functions. This discussion should include a description of each supervisory and managerial position, including the responsibilities and how lines of authority extend up to facility and corporate management.

#### 7. QUALITY ASSURANCE PROGRAMS

To provide assurance that the design and procurement of the physical protection system components for a plant are in conformance with applicable regulatory requirements and with the design bases and criteria specified in the license applications, an applicant should establish a Quality Assurance (QA) Program. Describe the QA Program to be established and executed for the physical protection system during the procurement, design, and construction stages.

If a portion of the QA Program to be implemented will conform to a particular quality assurance standard such as one adopted by the American National Standards Institute, the description may consist of a statement that the particular standard will be followed. Where regulatory guides have been issued on acceptable methods of implementing portions of the QA Program, the description should specifically indicate whether the regulatory positions of the regulatory guides will be followed.

#### 8. TESTING AND INSPECTION

Describe the programs to be implemented to regularly and periodically test and inspect all physical protection system components (equipment and design features) and procedures. Include a discussion of the management of these programs.

##### 8.1 Tests and Inspections During Installation

Describe the general procedures for conducting tests and inspections during installation and construction of physical-protection-related subsystems and components to ensure that they comply with their respective design criteria and performance specifications.

## 8.2 Preoperational Tests and Inspections

Describe the general procedures for conducting preoperational tests and inspections of physical-protection-related subsystems and components to demonstrate their effectiveness and availability with regard to their respective design criteria and performance specifications.

## 8.3 Operational Tests and Inspections

Identify the types of subsystems, number of zones, number of components, number of items tested each time, and the frequency and test procedure used to determine that physical-protection-related subsystems and components are in an operable and effective condition. Also indicate the functions performed in security force drills and the frequency and attendance of such drills. Information for this section may be displayed in tabular form.

## 9. MAINTENANCE PROGRAMS

Describe the programs to provide routine maintenance for all security-related equipment and design features and to provide emergency repair capabilities for both equipment and design features. Discuss the personnel who will perform these functions, including their training and qualifications, whether they are employees of the facility or contract personnel, and the lines of authority from facility management through security management to ensure continued effectiveness of these programs.

## 10. SECURITY AUDITS

Describe the programs to review periodically the applicability and adequacy of the existing Physical Protection Plan and to assess the compliance of the current performance with existing security requirements.

### 10.1 Program Audits

Describe the scope, extent, and frequency of planned periodic management audits to review the physical protection program of the facility for continued adequacy and effectiveness. Identify by organizational title the persons assigned responsibility for conducting the audits. Affirm that written audit reports will be prepared and submitted to facility management.

### 10.2 Compliance Audits

Describe the monitoring program established to ensure compliance with existing regulations. Identify by organizational title the persons assigned responsibility for conducting the audits. Affirm that written audit reports will be prepared and submitted to facility management.

## 11. SECURITY RECORDS

Describe the recordkeeping programs to provide compliance with the requirements of § 73.70.

### 11.1 Security Tours, Inspections, and Tests

Describe the system for documenting the results of all routine security tours and inspections and of all tests and inspections performed on physical barriers, intrusion alarms, communications equipment, and other security-related equipment.

### 11.2 Maintenance

Identify and characterize the records that are kept of all maintenance performed on physical barriers, intrusion alarms, communications equipment, and other security-related equipment.

### 11.3 Alarm Annunciations

Describe the records system for documenting all alarm annunciations, including false alarms. Also describe the system for identifying the type of alarm, location, date, and time of each occurrence.

### 11.4 Security Response

Indicate the records that are kept of response by facility guards and watchmen to each alarm (including false alarms), intrusion, or other security incidents.

### 11.5 Authorized Individuals

Describe the system for maintaining a record of each individual who is designated as an authorized individual. Indicate whether the record will include the name and badge number of each person so designated, the person's address, the date of the authorization, its expiration date, the name of the approval authority, and the areas to which access is authorized.

### 11.6 Nonemployee Access

Describe the system for maintaining a record (register) of each visitor, vendor, or other individual who is not an employee of the applicant, with the record showing the person's name; the date, time, and purpose of the visit; the person's employment affiliation and citizenship; the name and badge number of the escort; the name of the person to be visited; and the name of the person who authorized or approved the visit. Describe the system for maintaining a list of designated escorts.

## 12. REPORTS TO NRC

### 12.1 Incidents

Describe the procedures for reporting to NRC any incident in which an attempt has been made, or is believed to have been made, to commit a theft or unlawful diversion of SNM or to commit an act of radiological sabotage.

### 12.2 Unusual Occurrences

Describe procedures, if different from those of Section 12.1, for reporting to the NRC any unusual occurrences (such as civil disturbances, bomb threats, significant

vandalism, and demonstrations or strikes) that may or could have an effect on plant security.

### 12.3 Protection Plan Changes

Describe procedures for furnishing to the NRC reports of changes made in the Physical Protection Plan.

## 13. SCHEDULE FOR IMPLEMENTATION

Describe the schedule for implementing the Physical Protection Plan, with special attention to those portions involving new construction, significant physical modification of existing structures, or major equipment installation that will require extensions of time.

## 14. REDUNDANCY AND DIVERSITY

Identify the portions of the facility physical protection system for which redundant and diverse components are necessary in order to ensure adequate performance as provided for in paragraph 73.20(b)(2). In general terms, describe the subsystems and components to be used to provide this redundancy and diversity and the ways in which these subsystems and components are redundant and diverse.

## 15. PHYSICAL PROTECTION SYSTEM INTEGRITY

Describe how the physical protection system will be designed to ensure that the integrity of the system is maintained at all times and how the system will exhibit continued resistance to vulnerabilities. This is to be a generic discussion of the problem and of the techniques adopted to address it, with only a general description of the measures to be used, not a description of the specific components involved (such as the specific line supervisory or tamper-indicating circuitry that will be installed).

## 16. PHYSICAL PROTECTION SYSTEM POWER SOURCES

Describe the power sources to be used for all physical-protection-related systems and equipment, including an evaluation of the reliability and vulnerability of each power source. Describe the different emergency power systems (uninterruptible power or other backup power sources) to be provided to ensure that a power failure will not significantly degrade the physical protection system capabilities. This discussion should focus on the power sources as complete systems rather than viewing them from the perspective of the individual types of equipment to be powered (which will be addressed in Part II of the Protection Plan).

## 17. ALARM STATIONS

Describe the Central Alarm Station (CAS) and the Secondary Alarm Station (SAS) to be installed at the facility. Include their locations on the facility map. Provide a generic discussion of the CAS and the SAS that includes all those topics mentioned in the following paragraph. It will not be necessary to discuss individual components in detail since this information will be provided by the responses to the Components and Measures Information Request Sheets for the CAS and the SAS found in Appendix 1.

Describe the type of physical barriers and protective features to be used in the construction of the CAS and the SAS. Identify the equipment and procedures to be used at the CAS and the SAS for receiving, assessing, and recording alarm information. Describe the components to be used for communication with security force personnel, onsite response personnel, and other facility personnel and offices. Describe the components to be used for communication with offsite response personnel. Identify the power sources and security programs to be used to ensure the continuing operation of the equipment in the CAS and the SAS (refer to Chapters 15 and 16 as appropriate). Describe the procedures for granting access to the CAS and the SAS. Describe the command and control personnel and all other personnel who will staff the CAS and the SAS. Describe all activities to take place in the CAS and the SAS under Sections 17.1 and 17.2, respectively.

17.1 Central Alarm Station

17.2 Secondary Alarm Station

**PART II**

**SPECIFIC SYSTEM PERFORMANCE**

Part II consists of six chapters, Chapters 18 through 23, which parallel the structure of the performance capabilities in § 73.45 of the Physical Protection Upgrade Rule. The information to be provided in this section of the facility Physical Protection Plan should describe how the facility physical protection system provides the performance capabilities required in § 73.45. These descriptions should be of two types: (1) a general description of how the given capability is to be achieved and (2) an identification of the specific physical protection components and measures used to implement such a system. For each component and measure identified, the information specified on the Information Request Sheets of Appendix 1 should be provided.

Equipment descriptions should include manufacturer and model, when appropriate. In the case of design features such as walls and entry control portals, a basic physical description of the construction or structure should be provided. For procedures, a basic description of the security force actions that constitute the particular procedure should be provided. When a component or configuration of components is used more than once for the same physical protection purpose (for instance, at more than one portal), it is only necessary to provide the appropriate information once (and complete only one Information Request Sheet). The information can then be referenced. In the case of those components for which an Information Request Sheet is not provided, a description of the component at a level of detail comparable to that of the Components and Measures Information Request Sheets should be given.

Information necessary for the NRC to perform collusion analysis of protection plans is identified by asterisks in the Information Request Sheets. The following definitions pertain to those information requests:

Personnel "categories": These categories are groupings of facility personnel such that all members of one group have the same "access" or "control" privileges. Examples: plant management, security guards, visitors, safeguards maintenance personnel, process workers.

"Access" privilege: An "access" privilege gives personnel the capability to pass a given safeguard without being subject to the normal response afforded by that safeguard. Examples: the capability of a security guard to pass through a weapons detector while wearing a weapon and the subsequent detector alarm being ignored; the capability of certain personnel with NRC or DOE material access authorization to exit a material access area without being searched.

"Control" privilege: A "control" privilege gives personnel control or influence over a given safeguard, thereby producing the capability to neutralize that safeguard. Examples: the capability to physically turn off a safeguard; the capability to neutralize an alarm by ignoring it or authorizing others to ignore it; the capability to neutralize a safeguard through tampering with the component, power supply, or other support systems.

All redundant and diverse subsystems or components should be identified as such when they are described, with a statement of how these subsystems or

components provide redundancy and diversity. The criterion for determining the need for redundancy and diversity is: whenever a single adversary action could otherwise so degrade the subsystem or system as to disrupt the required performance capability. Several types of subsystems and systems should possess redundancy and diversity. These include most alarm and detection systems, certain communications links without which effective notification and response communications would not be possible, and alarm stations (a Central Alarm Station [CAS] and a Secondary Alarm Station [SAS]).

Certain portions of Chapters 20 and 21 of Part II contain areas of mutual concern to both material control and physical protection. Updated physical protection requirements in these areas will impact a licensee's Fundamental Nuclear Material Control (FNMC) Plan. In conjunction with the development of the Physical Protection Plan in response to the Upgrade Rule, the licensee should review his FNMC plan for consistency in these areas and submit to the NRC, concurrent with the protection plan submittal, any necessary revisions to the FNMC. FNMC areas probably requiring updating include organizational responsibilities, material accounting records and reports, storage and internal controls, and management reviews and audits.

#### 18. PREVENT UNAUTHORIZED ACCESS OF PERSONS AND MATERIALS INTO MATERIAL ACCESS AREAS AND VITAL AREAS

Describe the purpose and objective of the measures used to prevent unauthorized access to material access areas (MAAs) and vital areas (VAs). Relate these to the required performance capabilities of § 73.45(b).

##### 18.1 Entry Control Through MAA and VA Entry Portals

For each MAA and each VA, identify the number, location, and type of entry portals, referring to the facility map as appropriate. Treat each vault for SSNM storage as though it were a separate MAA, even though the vault is considered an item control area within an MAA and is located entirely within the MAA. For each portal, identify and describe all the components and measures required for the entry control functions presented in the following paragraphs. However, in cases where the same configuration of components is to be used at more than one entry portal, the measures need be described only once and may thereafter be referenced.

##### 18.1.1 Entry Authorization Procedures

Describe the development of entry authorization procedures. Discuss how the lists of authorized personnel for each portal will be developed. Also describe the distribution and maintenance of these lists.

##### 18.1.2 Entry Procedures and Controls for Routine Conditions

Describe how routine conditions differ between working and nonworking hours (nights, weekends, and holidays). Identify which portals are to be open and which are to be locked during each of these periods. This discussion should be related to the problem of entry in emergency situations, which are discussed in Section 18.1.3 below.

18.1.2.1 Procedures and Controls for Personnel Entry. For each entry portal, describe how the identification and authorization of each person is to be verified to prevent unauthorized access by deceit. Describe the policies and procedures to be used for the escort of visitors. Discuss the components to be used to detect contraband on authorized personnel at entry control points.

Discuss the procedures and equipment to be used by entry control personnel to notify command and control personnel of a suspected attempt at unauthorized entry. Identify the interim steps to be taken by entry control personnel in the period between notification of Security and the arrival of response personnel.

18.1.2.2 Procedures and Controls for Introduced Materials. Describe the components to be used to control the introduction of materials by deceit. Describe how the material entry authorizations are to be verified. Describe how the quantity and type of material is to be verified. These descriptions should include the components to be used in the detection of unauthorized materials that are hand carried by authorized individuals or mailed or otherwise shipped as part of an authorized shipment.

Describe the procedures and equipment to be used by the portal guard for the notification of command and control personnel in the event that the introduction of unauthorized materials is suspected. Identify the interim steps to be taken by access control personnel in the period between notification of Security and the arrival of response personnel.

18.1.2.3 Procedures and Controls for Introduction of Vehicles. Describe the procedures and equipment used to control the ingress of vehicles into MAAs and VAs, if applicable. Identify the components used to detect unauthorized materials on or in such vehicles, and relate this discussion to paragraph 18.1.2.2.

### 18.1.3 Entry Procedures and Controls for Nonroutine Conditions

Describe the components to be used for entry control during nonroutine conditions. Discuss how entry control personnel will verify that a bona fide nonroutine condition exists. Describe the procedures to be used for controlling the entry of personnel authorized to enter during each type of nonroutine condition if they differ from those described in paragraph 18.1.2.1.

Describe the procedures to be used for the escort of emergency personnel such as firefighters and ambulance assistants. Identify the procedures and equipment to be used by the portal guard to notify command and control personnel in the CAS and the SAS of a suspected attempt at unauthorized access during nonroutine conditions. Describe the interim actions to be taken between the notification of Security and the arrival of response personnel.

### 18.1.4 Bypass of Admittance Procedures and Controls

Describe the procedures and controls to be used to prevent unauthorized entry through portals by stealth or force (for both open and closed conditions at each portal). Describe the barriers and other components to be used to delay bypass attempts through the portal. Include a discussion of the components to be used to sense unauthorized entry attempts and transmit sensor data to Command and Control. Identify the equipment and procedures to be used at the CAS and

the SAS to assess the information. This discussion should include the identification of redundant and diverse components and subsystems to be used to ensure that the unauthorized entry is prevented.

Describe (in those cases where the portal is manned) the actions to be taken to prevent or delay the unauthorized entry attempt from succeeding in the interim between the notification of Security and the arrival of response personnel.

## 18.2 Entry Through Remainder of the MAA/VA Boundary

### 18.2.1 Detect Boundary Penetration Attempt

Describe the components to be used to detect attempts at unauthorized entry. Identify the components to be used to sense unauthorized entry attempts and to transmit sensor data to command and control personnel. Identify the equipment and procedures to be used at the CAS and the SAS to assess this information. This discussion should include the identification of redundant and diverse components and subsystems to be used to ensure that unauthorized entry is prevented.

### 18.2.2 Deter Boundary Penetration Attempt

Describe the barriers and other components to be used to prevent entry through the remainder of each MAA and each VA boundary (i.e., other than at the entry portals). Describe the physical barriers to be used at each MAA and each VA boundary. This description should address the construction of all walls, floors, and ceilings as well as how ventilation and other openings are to be secured.

### 18.2.3 Respond to Boundary Penetration Attempt

Describe the immediate actions to be taken between notification of Security and the arrival of response personnel. Identify the components to be used to contain unauthorized entry attempts sufficiently to permit the arrival of response forces who will prevent the attempt from succeeding.

## 19. PERMIT ONLY AUTHORIZED ACTIVITIES AND CONDITIONS WITHIN PROTECTED AREAS, MATERIAL ACCESS AREAS, AND VITAL AREAS

Describe the purpose and objective of the measures used to control activities and conditions. Relate these to the required performance capabilities of § 73.45(c).

### 19.1 Permit Only Authorized Activities and Conditions Within Protected Area

#### 19.1.1 Establishment of Authorized Activities and Conditions

Define the boundaries of the protected area (PA), referring to the facility map. Discuss the development of criteria to be used in defining those activities and conditions to be authorized and those to be prohibited. Describe how lists of authorized activities and conditions are to be developed, maintained, and distributed.

### 19.1.2 Prevention of Unauthorized Activities and Conditions

Discuss the components to be used to detect unauthorized activities and conditions, including those components to be used to sense unauthorized activities and conditions and to transmit sensor data to command and control personnel. Identify the equipment and procedures to be used at the CAS and the SAS to display the sensor data. This discussion should include the identification of redundant and diverse components and subsystems to be used. Describe any actions that security personnel who may detect unauthorized activities and conditions during routine patrols or tours will initiate in the interim between notification of command and control personnel and the arrival of response forces.

### 19.2 Permit Only Authorized Activities and Conditions Within MAA

In Sections 19.2.1 and 19.2.2, provide information for each MAA that is comparable to the information provided for PAs in Sections 19.1.1 and 19.1.2. However, in the case of multiple MAAs where the same configuration of components is to be used, it is not necessary to repeat the information. The information may be referenced.

#### 19.2.1 Establishment of Authorized Activities and Conditions

#### 19.2.2 Prevention of Unauthorized Activities and Conditions

### 19.3 Permit only Authorized Activities and Conditions Within VA

In Sections 19.3.1 and 19.3.2, provide information for each VA that is comparable to the information provided for PAs in Sections 19.1.1 and 19.1.2. However, in the case of multiple VAs where the same configuration of components is to be used, it is not necessary to repeat the information. The information may be referenced.

#### 19.3.1 Establishment of Authorized Activities and Conditions

#### 19.3.2 Prevention of Unauthorized Activities and Conditions

## 20. PERMIT ONLY AUTHORIZED PLACEMENT AND MOVEMENT OF SSNM WITHIN MAAs

Describe the purpose and objective of the measures used to control movement and placement of SSNM. Relate these to the required performance capabilities of § 73.45(d).

### 20.1 Establishment of Authorized Placement and Movement of SSNM

Describe the criteria to be used to delineate the authorized placement and movement of SSNM within each MAA. For each MAA, discuss the location(s) within the MAA for which the placement and movement of SSNM is to be authorized, referring to the facility map. Describe how schedules of authorized placement and movement of SSNM within each MAA are to be developed, maintained, and distributed.

## 20.2 Establishment of Current Knowledge of SSNM

For each MAA, describe the components to be used to verify the type, quantity and location of SSNM within the MAA. Discuss the procedures to be used to verify the authorization schedules. In the case of multiple MAAs where the same verification measures are to be used, this information may be referenced.

## 20.3 Prevention of Unauthorized Placement and Movement of SSNM

Describe the measures to be used to delay the unauthorized placement and movement of SSNM within each MAA (for example, the containment of SSNM within wire cages when it is between the vault and process machinery). Describe the components to be used to sense unauthorized placement or movement of SSNM and to transmit sensor data to command and control personnel. Identify the equipment and procedures to be used in the CAS and the SAS to assess sensor information. This discussion should include the identification of redundant and diverse components and subsystems to be used. For cases in which the unauthorized placement or movement of SSNM is detected by security personnel during routine patrol or escort operations, describe the actions to be taken by these security personnel in the interim between notification of command and control personnel and the arrival of response personnel.

## 21. PERMIT REMOVAL OF ONLY AUTHORIZED AND CONFIRMED FORMS AND AMOUNTS OF SSNM FROM MAAs

Describe the purpose and objective of the measures used to control removal of SSNM. Relate these to the required performance capabilities of § 73.45(e).

### 21.1 Control of SSNM Removal Through MAA Portals

For each MAA, identify the number, location, and type of portals, including reference to the facility map. For each portal, provide all information required in the following paragraphs. However, in cases where the same configuration of components is to be used at more than one portal, the measures need be described only once and may thereafter be referenced.

#### 21.1.1 Development of Removal Authorization Procedures

Describe the development of removal authorization procedures. Discuss how lists of authorized personnel are to be developed, distributed, and maintained.

#### 21.1.2 Removal Procedures and Controls for Normal Conditions

Describe how normal conditions differ between regular working hours and nonworking hours (nights, weekends, and holidays). Identify which portals are to be open and which are to be locked during each of these periods. In cases where authorized removal of SSNM, scrap, or waste may be limited to certain MAA portals, these portals should be identified in the appropriate paragraphs below.

21.1.2.1 Procedures and Control for SSNM Removal. For each portal, describe how the identification and authorization of each person presenting SSNM for removal from the MAA is to be verified to prevent removal by deceit.

Describe how the verification of authorization, type, and quantity of SSNM is to be confirmed. Discuss the components to be used to detect unauthorized removal of SSNM. Identify the components to be used to sense unauthorized attempts to remove SSNM from MAAs and to transmit sensor data to command and control personnel. Identify the equipment and procedures to be used at the CAS and the SAS to assess the sensor information. This discussion should include the identification of redundant and diverse components and subsystems to be used. Discuss the actions to be taken by the portal guard in the interim between notification of command and control personnel and the arrival of response personnel.

21.1.2.2 Procedures and Controls for Scrap Removal. For each portal, describe how the identification and authorization of each person presenting scrap material for removal is verified to prevent removal by deceit. Describe how the authorization, type, and quantity of scrap material is to be verified. Discuss the components and measures to be used to detect unauthorized removal of scrap. Identify the components to be used to sense unauthorized attempts to remove scrap from MAAs and to transmit sensor data to command and control personnel. Identify the equipment and procedures to be used at the CAS and the SAS to assess sensor information. This discussion should include the identification of redundant and diverse components and subsystems to be used. Discuss the actions to be taken by the portal guard in the interim between notification of command and control personnel and the arrival of response personnel.

21.1.2.3 Procedures and Controls for Waste Removal. For each portal, describe how the identification and authorization of each person presenting waste material for removal from the MAA is to be verified to prevent removal by deceit. Describe how the authorization, type, and quantity of waste material is to be verified. Identify the components to be used to sense unauthorized attempts to remove waste from MAAs and to transmit sensor data to command and control personnel. Identify the equipment and procedures to be used at the CAS and the SAS to assess sensor information. This discussion should include the identification of redundant and diverse components and subsystems to be used. Discuss the immediate actions to be taken by portal guards in the interim between notification of command and control personnel and the arrival of response personnel.

### 21.1.3 Removal Procedures and Controls Under Emergency Conditions

Describe the procedure by which emergency conditions are to be verified by security personnel at each portal. Describe the procedures and equipment to be used to verify the authorization of personnel attempting to remove SSNM, scrap, or waste during a bona fide emergency.

Discuss the procedures and equipment to be used by the portal guard to notify command and control personnel of a suspected attempt at unauthorized entry. Identify the interim steps to be taken by the portal guard in the period between notification of command and control personnel and the arrival of response personnel.

#### 21.1.4 Bypass of Removal Procedures

Describe the procedures and controls to be used to prevent unauthorized removal of SSNM, scrap, or waste by stealth or force (for both open and closed conditions at each portal). Describe the barriers and other components to be used to delay bypass attempts through the MAA portal. Discuss the components to be used to detect attempts to bypass removal procedures and controls. Include those components to be used to sense unauthorized removal attempts and to transmit sensor data to command and control personnel. Identify the equipment and procedures to be used at the CAS and the SAS to assess the information. This discussion should include the identification of redundant and diverse components and subsystems to be used. Identify the procedures and equipment to be used at manned portals in the interim between notification of command and control personnel and the arrival of response personnel.

#### 21.2 Removal of SSNM Through Remainder of Boundary

Describe the components to be used to prevent removal of SSNM through the remainder of the MAA boundary by means of stealth or force. Describe the barriers and other components to be used to prevent unauthorized removal of SSNM, including removal through ventilation, plumbing, and similar systems. Identify the components to be used to sense such attempts and to transmit sensor data to command and control personnel. Identify the equipment and procedures to be used at the CAS and the SAS to assess the information. This discussion should include the identification of redundant and diverse components and subsystems to be used. In the case of multiple MAAs where the same configuration of components is used, it is not necessary to repeat the information. The information may be referenced.

### 22. PROVIDE FOR AUTHORIZED ACCESS AND ASSURE DETECTION OF AND RESPONSE TO UNAUTHORIZED PENETRATIONS OF PA

Describe the purpose and objective of the measures used to control access to PAs. Relate these to the required performance capabilities of § 73.45(f).

#### 22.1 Entry Control Through PA Entry Portals

Identify the number, location, and type of entry portals in the PA, with reference to the facility map. For each portal, identify and describe all the components required for the entry control functions as requested in the following paragraphs. However, in cases where the same configuration of components is to be used at more than one entry portal, the measures need be described only once and may thereafter be referenced.

##### 22.1.1 Entry Authorization Procedures

Describe the development of entry authorization procedures. Discuss how lists of personnel, material, and vehicles authorized for entry into each portal will be developed. Describe the distribution and maintenance of these lists.

##### 22.1.2 Entry Procedures and Controls for Normal Conditions

Describe how normal conditions differ between regular working hours and nonworking hours (nights, weekends, and holidays). Identify which portals are

open and which are locked during each of these periods. This discussion should be related to the problem of entry in emergency situations, discussed in Section 22.1.3 below.

22.1.2.1 Procedures and Controls for Personnel and Vehicle Entry. For each entry portal, describe how the identification and authorization of each person and each vehicle is verified to prevent entry by deceit. Describe the policies and procedures used for the escort of visitors and offsite vehicles. Identify the methods used to detect, at entry control points, contraband on authorized personnel or in authorized vehicles. Describe the procedures and equipment to be used to notify command and control personnel in the event that entry control personnel suspect an attempt at unauthorized entry. Identify the steps to be taken by entry control personnel in the period between notification of command and control personnel and the arrival of response personnel.

22.1.2.2 Procedures and Controls for Introduced Materials. Describe the components to be used to control introduction of nuclear and nonnuclear materials by deceit. Describe how authorizations are to be verified. Describe how the quantity and type of materials are to be verified. Identify the components to be used to detect the introduction of unauthorized persons and materials that have been mailed, shipped, or carried on an authorized vehicle.

Describe the components to be used to notify command and control personnel in the event that introduction of unauthorized material is suspected. Identify the steps to be taken by entry control personnel in the period between notification of command and control personnel and the arrival of response personnel.

### 22.1.3 Procedures and Controls for Emergency Entry of Personnel and Vehicles

Describe the procedures and controls to be used for controlling entry during emergencies. Discuss how entry control personnel will verify that emergency conditions exist. Describe the procedures to be used for the escort of emergency personnel and emergency vehicles such as fire trucks and ambulances. Describe the procedures and equipment used to notify command and control and supervisory personnel in the event of an attempt at unauthorized emergency access. Describe the actions to be taken between the notification of command and control personnel and the arrival of response personnel.

### 22.1.4 Prevention of Bypass of Entry Procedures and Controls

Describe the procedures and controls to be used to prevent unauthorized entry through portals by stealth or force (for both open and closed conditions at each portal). Describe the barriers and other components to be used to delay bypass attempts through the entry portal. Include those components to be used to sense unauthorized entry and to transmit sensor data to command and control personnel. Identify the equipment and procedures to be used at the CAS and the SAS to assess this sensor information. This discussion should include the identification of redundant and diverse components and subsystems to be used. Describe the action to be taken by entry control personnel to prevent or delay the attempt from succeeding in the period between notification of command and control personnel and the arrival of response personnel.

## 22.2 Entry Through Remainder of PA Boundary

Describe the components to be used to prevent entry through the remainder of the PA boundary. Describe the physical barriers to be used at the boundary and the isolation zone. The description of physical barriers should address the construction of all fences and gates. For buildings that form part of the boundary, describe the construction of the walls, floors, and ceilings, as well as how ventilation and other openings are to be secured.

Describe the components to be used to detect attempts at unauthorized entry. Identify the components to be used to sense unauthorized entry attempts and to transmit sensor data to command and control personnel. Identify the equipment and procedures to be used at the CAS and the SAS to assess the sensor information. This discussion should include the identification of redundant and diverse components and subsystems to be used.

Describe the actions to be taken by security personnel who detect penetration attempts while on routine patrol, escort, or inspection operations between the time they notify command and control personnel and the arrival of response personnel. Identify the equipment and procedures to be used to contain unauthorized entry attempts sufficiently to prevent the attempt from resulting in theft of SNM or radiological sabotage.

## 23. RESPONSE

Describe the purpose and objective of response measures to be employed. Relate these to the required performance capabilities of § 73.45(g).

### 23.1 Communications

#### 23.1.1 Communications with Onsite Forces

Describe the equipment and procedures to be used by command and control personnel to communicate with onsite security and response forces (this description should be coordinated with the discussion of the makeup of the onsite force in Section 23.2.1 below). The information provided here should include all communications with onsite forces that take place after command and control personnel are notified of possible contingency conditions. Describe the equipment and procedures to be used by supervisory personnel to communicate response instructions to the onsite force if these differ from the ones previously described. This description should include identification of redundant and diverse components and subsystems to be used.

#### 23.1.2 Communications with Offsite Forces

Describe the equipment and procedures to be used by command and control personnel to communicate with offsite response forces (this description should be coordinated with the discussion of the makeup of the offsite forces in Section 23.2.2 below). Discuss communications with each local law enforcement agency involved in response activities and communications with all offsite response personnel other than local law enforcement agencies (for example off-duty employees). This discussion should include identification of redundant and diverse components and subsystems to be used.

## 23.2 Effective Response

This discussion should rely on, and to some extent summarize, information provided in the facility Contingency Plan. While that plan should be referenced for detail, this section should provide an adequate description of the response capabilities.

### 23.2.1 Onsite Response

Discuss the personnel who constitute the onsite response force, and describe their training (include security personnel and any nonsecurity personnel with response responsibilities). Reference the Guard Training Plan for training details. Describe the equipment and procedures to be used by onsite personnel in providing an effective response to each of the unauthorized situations discussed in the previous chapters. Explain how the use of this equipment and these procedures result in containment until the offsite response forces arrive.

### 23.2.2 Offsite Response

Discuss the local law enforcement agency personnel (and their training and equipment) who are to constitute the offsite response force. Also describe any other offsite response personnel who may be used for response actions. Include here the approximate time required for offsite forces to arrive at the facility after notification. Take into consideration possible weather conditions. (Also include here detailed aspects of the offsite response capability not discussed in Chapter 3 of Part I. If the discussion in Chapter 3 of Part I is already provided in substantial detail, it may simply be referenced.)

APPENDIX 1

COMPONENTS AND MEASURES LIST AND INFORMATION REQUEST SHEETS

A. PHYSICAL PROTECTION COMPONENTS AND MEASURES LIST

1. Admittance Authorization Criteria and Schedules
2. Admittance Authorization and Verification Procedures
3. Air and Utility Inlet Barriers
4. Annunciation Systems
  - Computer-Assisted
  - Individual Alarm
  - Multiplexed Alarm
5. Area Zoning
6. Balanced Magnetic Switches
7. Breakwire Systems
8. Buried-Line Sensors
  - Seismic
  - Magnetic
  - Geophone String
  - Piezoelectric String
9. Capacitance Alarms
10. CCTV Monitoring/Surveillance
11. CCTV Systems
12. Central and Secondary Alarm Stations
13. Close-out Inspection by Third Party
14. Coded Credential System
  - Active Electronic Badge Reader
  - Capacitance-Code Badge Reader
  - Electric-Circuit Badge Reader
  - Magnetic-Code Badge Reader
  - Magnetic-Strip Badge Reader
  - Metallic-Strip Badge Reader
  - Optical-Code Badge Reader
  - Passive Electric Badge Reader
15. Commercial Telephone System
16. Contingency Plans and Procedures
17. Controlled Security Lighting
18. Data Link via Radio Frequency
19. Direct-Line Telephone Intercom
20. Direct Monitoring/Surveillance
21. Doors and Associated Hardware
22. Duress Alarms
23. E-Field Fence
24. Electret Sensor and Tilt Switch Fence Systems
25. Emergency Access Procedures
26. Emergency Battery System
27. Emergency Evacuation Procedures
28. Emergency Exits
29. Emergency Generator Systems
30. Equipment Checks and Maintenance
31. Escorts

32. Explosive Detector
  - Hand-Held, Package Search
33. Explosive Detector
  - Hand-Held, Personnel Search
34. Explosive Detector
  - Hand-Held, Vehicle Search
35. Explosive Detector
  - Volume
36. Explosive Detector
  - Walk-Through
37. Fence Systems
38. Floors, Roofs, and Walls
39. Functional Zoning
40. Gates and Associated Hardware
41. Guard Force Personal Equipment
42. Guard Force Qualifications
43. Guard Patrols and Intervention
44. Guard Post Assignments
45. Hardwire Video Systems
46. Infrared Beam Systems, Exterior
47. Interface Between Alarm Station and Sensors
  - Individual Hardwire Alarms
  - Multiplexed Hardwire Alarms
  - Hardwire Command Signals
48. Isolation Zones
49. K-9s, Used for Package or Vehicle Search
50. Local Audible or Visible Alarms
51. Locks (Keyed, Keyless)
52. Manual Alarm Recording
53. Master (Fixed) Radio
54. Microwave Systems, Exterior
55. Mobile Radio
56. Motion Detectors
  - Interior Infrared Beam Systems
  - Interior Microwave Systems
  - Ultrasonic and Sonic Systems
57. Multi-Man Rule
58. Night Vision Devices
59. Pat-Down Search
60. Personal Identification Numbers and Passwords
61. Photo Identification Badges
62. Physical Controls and Procedures for Keys, Locks, Combinations, and Cipher Systems
63. Portable Radio
64. Positive Personnel Identity Verification
  - Fingerprints
  - Handwriting
  - Hand Geometry
  - Voice Prints
65. Response Vehicles
66. Sally Ports, Pedestrian
67. Sally Ports, Vehicle

- 68. Shielding Detectors
  - Volume
- 69. Shielding Detectors
  - Walk-Through
- 70. SNM Containers
- 71. SNM Detectors
  - Hand-Held, Package Search
- 72. SNM Detectors
  - Hand-Held, Personnel Search
- 73. SNM Detectors
  - Volume
- 74. SNM Detectors
  - Walk-Through
- 75. SNM Holding/Storage Areas
- 76. SNM Identification/Authorization Procedures
- 77. SNM Liquid and Solid Waste Handling Procedures
- 78. SNM Scrap Removal Procedures
- 79. SNM Shipping and Receiving Procedures
- 80. Tamper-Indicating Circuitry
- 81. Tamper-Indicating Seals and Tamper-Seal Inspection
- 82. Team Zoning
  - Two-Man Rule (see #57--Multi-Man Rule)
- 83. Uninterruptible Power Systems
- 84. Vaults
- 85. Vibration Sensors
- 86. Visual Inspection, Package Search
- 87. Visual Inspection, Vehicle Search
- 88. Weapons
  - Handgun
  - Semiautomatic
  - Shotgun
- 89. Weapons Detector
  - Hand-Held, Package and Personnel Search
- 90. Weapons Detector
  - Volume
- 91. Weapons Detector
  - Walk-Through
- 92. Windows and Associated Hardware
- 93. X-Ray Package and Container Search

B. PHYSICAL PROTECTION COMPONENTS AND MEASURES INFORMATION REQUEST SHEETS\*

1. ADMITTANCE AUTHORIZATION CRITERIA AND SCHEDULES

1. Describe what these criteria and schedules are expected to accomplish, indicating where and when they will be used.
2. List, by function, all personnel responsible for formulating and authorizing the criteria and schedules.
3. Identify verification or audit methods that ensure schedules are properly executed.
4. Outline the methods used for criteria development in granting admittance authorization, establishment and maintenance of admittance schedules, and organization of authorization papers and schedules for personnel, vehicles, and material.
5. Describe the methods used to deter collusion among personnel who are responsible for formulating and authorizing the criteria and schedules.

2. ADMITTANCE AUTHORIZATION AND VERIFICATION PROCEDURES

1. Describe what these procedures are expected to accomplish, indicating when and where they will be used.
2. List, by function, the personnel who perform the authorization and verification procedures, describing how these personnel are selected, and the personnel responsible for the selection.
3. Describe the training that personnel receive in performing the procedure.
4. Identify verification or audit methods that ensure procedures are properly executed.
5. Outline how admittance verification is conducted for facility employees, visitors, vehicles, and material. List the type of information required on admittance authorization and verification records. Indicate any varying levels of admittance authorization and verification that are dependent on employee access.
6. Describe the methods used to deter collusion among personnel who are involved with the procedures.
- \*7. Identify by personnel category all facility employees and others who have control of this safeguard.

\* See p. 5.52-11 of Part II, "Specific System Performance," for the definitions needed to answer the questions marked with asterisks.

### 3. AIR AND UTILITY INLET BARRIERS

1. Describe all air and utility inlet barriers, including what area they are in, where they are located within the building structure, size, construction, and where and at what height the inlet initiates and terminates.
2. Describe the reasons for installing the barriers and measures taken to ensure that any inlets without barriers are adequately protected.
3. Indicate what materials or components will be vulnerable through unauthorized use of the inlet.
4. Identify the physical protection components and measures, including personnel functions, used to monitor or provide security for the inlet and barrier. Describe where and how any alarms annunciate.
5. Describe the known or anticipated vulnerabilities of the inlet barriers, and indicate how they will be compensated for.

### 4. ANNUNCIATION SYSTEMS

- Computer-Assisted
- Individual Alarm
- Multiplexed Alarm

1. Describe the type of annunciation system, including identification of all critical components, their location, and their function within the annunciation system.
2. Describe system operation, how information is presented and in what priority, how events are assessed and recorded, and what procedures are used to ensure effective operation.
3. Describe the installation, including how system controls and displays are laid out. If installation differs from manufacturer's recommendations, specify how and why.
4. Indicate the type and duration of backup power available.
5. Describe backup equipment or procedures to be used in the event of system failure.
6. Describe the frequency and kind of preventive maintenance and operational testing.
7. Describe tamper protection and line supervision used with the system, including program change protection or access controls used with computer-assisted systems.
8. Describe operator training in the use of the system.
- \*9. Identify by personnel category all facility employees and others who have control of this safeguard.

## 5. AREA ZONING

1. Describe what area zoning is expected to accomplish, indicating where and when it will be used. Reference facility maps as required.
2. List, by function, personnel who work within zoned areas and personnel responsible for assigning duties.
3. Identify the training that personnel will receive in proper area zoning procedures.
4. Identify verification or audit methods that ensure area zoning is properly executed.
5. Outline the work rules that have been established in conjunction with area zoning. Indicate any restrictions placed on individuals working within one area zone or multiple zones and whether individuals may rotate duties within or between zones.

## 6. BALANCED MAGNETIC SWITCHES.

1. Describe the type of balanced magnetic switches used, their location, and what they protect. Specify switch movement distance necessary to initiate an alarm.
2. Describe the installation, including location of control or processing units. If installation differs from manufacturer's recommendations, specify how and why.
3. Indicate where the alarm annunciates, how an alarm condition is assessed, and what response occurs when an alarm is indicated.
4. If applicable, indicate the type and duration of backup power available.
5. Identify any other physical protection components or subsystems that provide direct redundant or backup protection in the event of switch failure.
6. Describe tamper protection and line supervision used with the alarm.
7. Describe the frequency and kind of preventive maintenance and operational testing. Include any available data on mean time between failures.
8. Discuss any known or anticipated vulnerabilities of the switches, and indicate how they will be compensated for.
- \*9. Identify by personnel category all facility employees and others who have access past this safeguard.
- \*10. Identify by personnel category all facility employees and others who have control of this safeguard.

## 7. BREAKWIRE SYSTEMS (FOIL STRIP AND GRID WIRE)

1. Describe the type of breakwire system used, its location, and what it protects.
2. Describe the installation, including location of control or processing units, and how the foil or wire is patterned to provide adequate coverage. If installation differs from manufacturer's recommendations, specify how and why.
3. Indicate where the alarm annunciates, how an alarm condition is assessed, and what response occurs when an alarm is indicated.
4. Describe the type and duration of backup power available.
5. Identify any other physical protection system components or subsystems that provide direct redundant or backup protection in the event of alarm failure.
6. Describe tamper protection and line supervision used with the alarm.
7. Describe the frequency and kind of preventive maintenance and operational testing. Include any available data on mean time between failures.
- \*8. Identify by personnel category all facility employees and others who have access past this safeguard.
- \*9. Identify by personnel category all facility employees and others who have control of this safeguard.

## 8. BURIED-LINE SENSORS

- Seismic
- Magnetic
- Geophone String
- Piezoelectric String

1. Describe the type of buried line sensor used, its location, and what it protects. Indicate its detection sensitivity in terms of intruder size, speed, and mode of advancement and reliability in terms of probability of detection and false alarm rate.
2. Describe characteristics of the area in which the sensor is installed that could lessen effective operation, including man-made or natural conditions such as vehicle activity or sources of electromagnetic interference. Indicate how nuisance alarms from such sources will be minimized.
3. Describe the installation, including location of control or processing units. If installation differs from manufacturer's recommendations, specify how and why.
4. Indicate where the alarm annunciates, how an alarm condition is assessed, and what response occurs when an alarm is indicated.

5. Describe the type and duration of backup power available.
6. Identify any other physical protection system component or subsystem that provides direct redundant or backup protection in the event of alarm failure.
7. Describe the frequency and kind of preventive maintenance and operational testing. Include any available data on mean time between failures.
8. Describe tamper protection and line supervision used with the alarm.
- \*9. Identify by personnel category all facility employees and others who have access past this safeguard.
- \*10. Identify by personnel category all facility employees and others who have control of this safeguard.

#### 9. CAPACITANCE ALARMS

1. Describe the type of capacitance alarm used, its location, and what it protects. Indicate its detection sensitivity in terms of intruder size, speed, and mode of advancement and reliability in terms of probability of detection and false alarm rate.
2. Describe characteristics of the area in which the alarm is located that could lessen effective operation such as other objects located nearby, the level of activity in the area, and nearby sources of electromagnetic interference. Also indicate any significant environmental conditions such as frequent thunderstorms or seismic activity that may have an adverse effect on alarm operation. Identify measures used to compensate for such characteristics.
3. Describe the installation, including location of control or processing units and how sensor grounding is provided. If installation differs from manufacturer's recommendations, specify how and why.
4. Indicate where the alarm annunciates, how an alarm condition is assessed, and what response occurs when an alarm is indicated.
5. Describe the type and duration of backup power available.
6. Identify any other physical protection system component or subsystem that provides direct redundant or backup protection in the event of alarm failure.
7. Describe tamper protection and line supervision used with the alarm.
8. Describe the frequency and kind of preventive maintenance and operational testing. Include any available data on mean time between failures.
- \*9. Identify by personnel category all facility employees and others who have access past this safeguard.
- \*10. Identify by personnel category all facility employees and others who have control of this safeguard.

## 10. CCTV MONITORING/SURVEILLANCE

1. Describe the type of CCTV monitoring system used, its location, and what facility areas it monitors. Include a list of primary equipment. Specify capability and operation, including coverage and blind spots, where and by whom it is monitored, how controls and monitors are grouped, screen size and spatial relationship between equipment and operators, length of operator shifts and break periods, whether observation is continuous or periodic, and number of screens monitored per operation.
2. Describe the installation. If installation differs from manufacturer's recommendations, specify how and why.
3. Describe the type and duration of backup power.
4. Identify any other physical protection system component or subsystem that provides direct redundant or backup capability in the event of system failure.
5. Describe the frequency and kind of preventive maintenance and operational testing. Include any available data on mean time between failures.
6. Describe operator training in CCTV monitoring and surveillance.

## 11. CCTV SYSTEMS

1. Describe the type of system used, its location, and its function (e.g., periodic or continuous observation, alarm assessment, motion detection and observation). Describe expected performance in terms of resolution and lighting provided to achieve resolution specifications.
2. Describe area characteristics that could lessen effective operation, including man-made and environmental conditions. Identify measures used to compensate for such problems.
3. Describe the installation, including location of and protection afforded all critical components. If installation differs from manufacturer's recommendations, specify how and why.
4. Indicate where the system is monitored, how an abnormal condition is assessed, and what response occurs when an abnormal condition is identified.
5. Describe the type and duration of backup power.
6. Identify any other physical protection system component or subsystem that provides direct redundant or backup protection in the event of system failure.
7. Describe tamper protection and line supervision used with the system.
8. Describe the frequency and kind of preventive maintenance and operational testing. Include any available data on mean time between failures.
- \*9. Identify by personnel category all facility employees and others who have access past this safeguard.

- \*10. Identify by personnel category all facility employees and others who have control of this safeguard.

## 12. CENTRAL AND SECONDARY ALARM STATIONS

1. Describe the functions of the central alarm station (CAS) and secondary alarm station (SAS) and using a map, if necessary, indicate the location of both.
2. Describe the construction of the two stations, indicating hardening techniques used in the construction and identifying the extent to which the CAS and the SAS are redundant.
3. List all personnel, by function, with access to the CAS and the SAS. Indicate who has control over the station during normal and emergency conditions. Describe the training that personnel receive in proper alarm station operating procedures.
4. Identify verification or audit methods that ensure procedures are properly executed.
5. Outline the operational activities performed by both the CAS and the SAS. List the primary equipment comprising the security systems of each station. Briefly describe the communications network among the CAS, SAS, and the offsite and onsite forces. Fully describe all recordkeeping procedures. Indicate the procedures used to gain authorized entry into the CAS and the SAS. Identify whether each station will be continuously manned and monitored. State whether the status of alarms can be changed in one station without notification or indication in the other, and describe CAS and SAS procedures during emergency situations, highlighting the differences from normal situations.
6. Highlight the methods used to minimize collusion among station operators.

## 13. CLOSE-OUT INSPECTION BY THIRD PARTY

1. Describe what a close-out inspection by a third party is expected to achieve. Indicate where and how it will be used and how soon after repair and maintenance it will be accomplished.
2. List all personnel, by function, who perform the inspection, describing how these personnel are selected and person(s) responsible for the selection.
3. Describe the instruction that personnel will receive in performing close-out inspections.
4. Identify the verification or audit methods that ensure that close-out inspections are properly executed.
5. Outline how a close-out inspection is performed.

#### 14. CODED CREDENTIAL SYSTEM

- Active Electronic Badge Reader
- Capacitance-Code Badge Reader
- Electric-Circuit Badge Reader
- Magnetic-Code Badge Reader
- Magnetic-Strip Badge Reader
- Metallic-Strip Badge Reader
- Optical-Code Badge Reader
- Passive Electric Badge Reader

1. Describe the type of system, its location, and its intended purpose within the physical protection system (e.g., ID, personnel tracking).
2. Describe the system's capabilities and standard operating procedures. Indicate whether credentials will remain on site or be retained by exiting personnel. Describe the type of "false" credentials to which the system might be vulnerable.
3. Describe credential issuance, auditing, accounting, retrieval, and destruction procedures.
4. Describe redundant equipment or procedures used in the event of system failure.
5. Describe the frequency and kind of preventive maintenance and operational testing. Include the individuals, by function, who perform the maintenance and testing.
6. Describe tamper protection and line supervision used with the system.

#### 15. COMMERCIAL TELEPHONE SYSTEM

1. Identify the physical protection communications functions performed by the system. If a central switchboard is used, describe its location and the protection afforded it. Identify frame-room locations and protection afforded them.
2. Describe redundant communications equipment or procedures that can be used in the event of system failure.

#### 16. CONTINGENCY PLANS AND PROCEDURES

1. Describe what contingency plans and procedures are expected to achieve, and indicate any of their discrepancies from the requirements of Appendix C to 10 CFR Part 73.
2. Describe how the security force and other pertinent personnel will be trained and kept familiarized with the contingency plans and procedures.
3. Identify verification or audit methods that ensure that contingency plans are properly executed in the event of a contingency.

## 17. CONTROLLED SECURITY LIGHTING

1. Describe the function of controlled security lighting. Using a map if necessary, describe where the controlled security lighting is located within the facility and its area of coverage. This should include location of lamps, junction boxes, cables, controls, etc. Describe the type of lighting used and illumination levels produced.
2. List all personnel, by function, with control over the lighting.
3. Indicate the physical protection components that are used to monitor or provide backup security for this component. Describe how the system will be powered in case of normal power failure, indicating what percentage of the system will be powered, and for how long, by the emergency power system. Indicate whether the power supply system is uninterruptible and, if not, state the time required to restore lighting. Identify any tamper-indicating or line-supervisory technique associated with the system.
4. Describe the planned maintenance and testing procedures for the lighting, and identify personnel, by function, who will perform maintenance and testing.
5. Discuss any known or anticipated vulnerabilities of the system such as blind spots, and indicate how they will be compensated for.

## 18. DATA LINK VIA RADIO FREQUENCY

1. Describe the type of link used, the type of communications it carries, the frequencies used, where transmitted information originates and terminates, and what physical protection system purpose is served by the link.
2. Describe area characteristics, man made or environmental, that could lessen effective operation. Describe methods used to compensate for such characteristics.
3. Describe the installation. If installation differs from manufacturer's recommendations, specify how and why.
4. Identify redundant communication equipment that could perform this function in the event of data link failure.
5. Describe the frequency and kind of preventive maintenance and operational testing.
6. Describe tamper protection used with the equipment.

## 19. DIRECT-LINE TELEPHONE INTERCOM

1. Describe the type of system, its locations, and what communications purpose it serves.
2. Describe the type and duration of backup power.

3. Identify redundant safeguards system components or subsystems that can be used in the event of telephone intercom failure.
4. Describe the frequency and kind of preventive maintenance and operational testing.

## 20. DIRECT MONITORING/SURVEILLANCE

1. Describe the conditions and situation under which direct monitoring/surveillance will be used. Indicate the areas that will be monitored in this manner under normal and nonnormal conditions.
2. List all personnel, by function, who will perform the direct monitoring/surveillance. Specify how the observers will be assigned duties and who will assign duties.
3. Describe the instructions that observers will receive for monitoring an area.
4. Identify verification or audit methods that ensure procedures are properly executed.
5. Outline how the direct monitoring/surveillance will be performed. This should specify how long the monitoring and break periods will be, other tasks that the observer will perform simultaneously with monitoring, and how the monitoring will be recorded and documented.
6. Describe the methods used to deter collusion among personnel who perform the direct monitoring/surveillance, specifying the degree to which assignments are random and how far in advance monitoring duties are assigned.
- \*7. Identify by personnel category all facility employees and others who have access past this safeguard.
- \*8. Identify by personnel category all facility employees and others who have control of this safeguard.

## 21. DOORS AND ASSOCIATED HARDWARE

1. State the function of the door(s) and describe what it protects. Describe the door(s) in terms of type of material used, door thickness, type of frame and how anchored to the wall, type of hinges and how attached, and the locking mechanism used. Indicate both the location of the door within the facility and the expected penetration delay time of the door and its associated hardware. (Calculations of penetration delay time are discussed in the Sandia Barrier Handbook.)
2. Indicate the physical protection components and measures (including personnel functions) used to monitor or provide security for the component. This should indicate the type of alarm sensor installed, if any, and the method used to assess an alarm condition.

3. Describe the known vulnerabilities of the door and methods used to compensate for them.

## 22. DURESS ALARMS

1. Describe the type of duress alarm used, its location if fixed, and whom (by job function) it is intended to protect. Specify performance characteristics in terms of how the alarm is actuated, how an alarm signal is transmitted, what an alarm signifies (e.g., alarm/normal capability only, coded alarm signal specifying more than one type of alarm condition), and false alarm rate.
2. If the alarm is of the radio frequency (RF) transmission type, describe facility or area characteristics that could lessen effective operation and measures used to compensate for such characteristics.
3. Describe the installation, if applicable. If the installation differs from manufacturer's recommendations, specify how and why.
4. Indicate where the alarm annunciates, how an alarm condition is assessed, and what response occurs when an alarm is indicated.
5. Describe the type and duration of backup power available.
6. Identify any other physical protection system component or subsystem that provides direct redundant or backup protection in the event of alarm failure.
7. Describe tamper protection and line supervision used with the alarm.
8. Describe the frequency and kind of preventive maintenance and operational testing. Include any available data on mean time between failures.

## 23. E-FIELD FENCE

1. Describe the E-field fence system, its location, and what it protects. Indicate its detection sensitivity in terms of intruder size, speed, and mode of advancement and reliability in terms of probability of detection and false alarm rate.
2. Describe area characteristics, either man made or environmental, that could lessen effective operation and measures used to compensate for such characteristics.
3. Describe the installation, including location of control or processing units. If the installation differs from manufacturer's recommendations, specify how and why.
4. Indicate where the alarm annunciates, how an alarm condition is assessed, and what response occurs when an alarm is indicated.
5. Describe the type and duration of backup power available.

6. Identify any other physical protection system component or subsystem that provides direct redundant or backup protection in the event of alarm failure.
7. Describe tamper protection and line supervision used with the alarm.
8. Describe the frequency and kind of preventive maintenance and operational testing. Include any available data on mean time between failures.
- \*9. Identify by personnel category all facility employees and others who have access past this safeguard.
- \*10. Identify by personnel category all facility employees and others who have control of this safeguard.

#### 24. ELECTRET SENSOR AND TILT SWITCH FENCE SYSTEMS

1. Describe the type of sensor used, its location, and what it protects. Indicate its detection sensitivity in terms of intruder size, speed, and mode of advancement and reliability in terms of probability of detection and false alarm rate.
2. Describe area characteristics, either man made or environmental, that could lessen effective operation. Identify measures used to compensate for such characteristics.
3. Describe the installation, including location of control or processing units and a description of any fencing used in conjunction with the systems. If the installation differs from manufacturer's recommendations, specify how and why.
4. Indicate where the alarm annunciates, how an alarm condition is assessed, and what response occurs when an alarm is indicated.
5. Describe the type and duration of backup power available.
6. Identify any other physical protection system component or subsystem that provides direct redundant or backup protection in the event of alarm failure.
7. Describe tamper protection and line supervision used with the alarm.
8. Describe the frequency and kind of preventive maintenance and operational testing. Include any available data on mean time between failures.
- \*9. Identify by personnel category all facility employees and others who have access past this safeguard.
- \*10. Identify by personnel category all facility employees and others who have control of this safeguard.

## 25. EMERGENCY ACCESS PROCEDURES

1. Describe the objectives of emergency access procedures, stating how, when, and where they are initiated in response to fire, medical, or criticality alarms.
2. List the personnel, by function, who are directly involved in the procedure, indicating who performs verification and escort duties, how these duties are assigned, and the personnel responsible for assigning duties.
3. Describe the training that personnel will receive in handling emergency access situations.
4. Identify verification, audit, or escort methods used to ensure that emergency access procedures are properly executed.
5. Outline all procedures associated with emergency access. Include information on verification methods, degree of screening or searches performed on material or personnel, and locations of emergency vehicles (if located within the facility).
6. Describe methods used to deter collusion among personnel who control the emergency access procedures.

## 26. EMERGENCY BATTERY SYSTEM (EBS)

1. State the purpose and function of the EBS. Indicate the location of the EBS, and describe the type of EBS to be used. Indicate the physical protection components that comprise the load, the length of time the barriers are capable of carrying the load, how the load will be carried if the power outage exceeds this time, and the amount of time required to recharge the batteries to 90 percent of full charge after being fully discharged.
2. Describe any environmental conditions present that may be detrimental to EBS operation.
3. Describe the physical protection components and measures (including personnel functions) used to monitor or provide security for the component.
4. Indicate the known or anticipated vulnerabilities of the system and how they will be compensated for.

## 27. EMERGENCY EVACUATION PROCEDURES

1. Describe the objectives of emergency evacuation procedures, stating how, when, and where they are initiated.
2. List the personnel, by function, who are directly involved in the procedure. Indicate how specific duties are assigned and the personnel responsible for assigning them.

3. Describe the training that personnel will receive in handling emergency evacuation procedures.
4. Identify verification, audit, or escort methods used to ensure that emergency evacuation procedures are properly executed and "false" evacuations deterred.
5. Outline how an emergency evacuation is initiated and performed. Describe all emergency evacuation routes and centers and methods for channeling personnel. Indicate how the passing or tossing of contraband outside the protected area (PA) will be prevented.
6. Describe methods used to deter collusion among personnel who control emergency evacuation procedures.

## 28. EMERGENCY EXITS

1. Describe the type of emergency exit used and its intended purpose. Indicate the location of all emergency exits with respect to material access areas (MAAs), vital areas (VAs), and PAs, referring to maps and drawings as necessary.
2. Describe the emergency exit in terms of its type, thickness, type of frame and how anchored to the structure, type of hinges used and how attached, and the locking mechanism used. Indicate the expected penetration delay time, with consideration given to all component parts of the exit.
3. Indicate other physical protection components and measures (including personnel functions) used to monitor or provide backup security for this component. A description of the type of alarms installed, how the alarms are activated, where an alarm condition is annunciated (local, remote), and type of annunciation (audible, visible) should be included. Also describe the type of tamper seals used, if any, and the manner in which the seals are applied. Indicate the frequency and manner in which the alarms are tested and the seals are verified and the personnel, by function, responsible for the testing and verification.
4. Describe the known vulnerabilities of the emergency exits and how they will be compensated for. Identify the area into which the exit leads, and describe the measures to be taken to ensure that no material is removed while the exit is open. Describe the assessment methods and the personnel, by function, employed to assess an alarm condition.
- \*5. Identify by personnel category all facility employees and others who have access past this safeguard.
- \*6. Identify by personnel category all facility employees and others who have control of this safeguard.

## 29. EMERGENCY GENERATOR SYSTEMS (EGS)

1. State the purpose and function of the EGS.

2. Describe any environmental conditions that may be detrimental to the EGS operations.
3. Describe the physical protection components and measures (including personnel functions) used to monitor or provide security for the component.
4. Describe the method to be followed in functionally testing the system. Indicate the frequency of such tests. Also indicate the frequency of routine and preventive maintenance and the level of training given maintenance personnel. Describe, by function, all personnel who perform testing and maintenance on the system. Indicate provisions made for alternative sources of backup power during maintenance periods.
5. Indicate the known or anticipated vulnerabilities of the system and how they will be compensated for.

### 30. EQUIPMENT CHECKS AND MAINTENANCE

1. Describe what equipment checks and maintenance procedures are expected to achieve and where and how they will be used.
2. List all personnel, by function, who perform the procedure, describing how these personnel are selected and the person(s) responsible for the selection.
3. Describe the training that personnel will receive in performing the procedure.
4. Identify the verification or audit methods that ensure that equipment checks and maintenance are properly executed. Describe recordkeeping procedures.
5. Describe methods used to deter collusion among personnel who perform equipment checks and maintenance.

### 31. ESCORTS

1. Describe the function of the escorts. List all categories of personnel or vehicles requiring escort and the general areas to which they are permitted access with escort. Indicate how identification of persons requiring escort will initially be verified and how these persons will be identified within the facility.
2. Outline the training received by escorts to help them perform their duties, indicating whether or not the escort is armed.
3. Identify the personnel who assign escort duties. Indicate how far in advance these duties are assigned and whether they are posted.
4. Indicate the procedures used in assigning escort duties, describing whether duties are assigned randomly or on a rotating basis and what measures will be taken to prevent collusion between an escort and an outsider.

32. EXPLOSIVE DETECTOR  
- Hand-Held, Package Search

1. Describe the type of detector, where it is used, and its performance specifications in terms of type and quantity of material that can be detected, probability of detection, and false alarm rate.
2. Describe detector operation, including how the search is to be conducted and what procedures (including response) are followed in the event of an alarm. Identify the training an operator receives in conducting the search.
3. Identify any area characteristics, e.g., air contamination, that could lessen effective operation, and describe means used to compensate for such characteristics.
4. Describe redundant physical protection components or procedures that can be used to perform this function in the event of detector failure.
5. Describe the frequency and kind of preventive maintenance and operational testing.
- \*6. Identify by personnel category all facility employees and others who have access past this safeguard.
- \*7. Identify by personnel category all facility employees and others who have control of this safeguard.

33. EXPLOSIVE DETECTOR  
- Hand-Held, Personnel Search

1. Describe the type of detector, where it is used, and its performance specifications in terms of type and quantity of material that can be detected, probability of detection, and false alarm rate.
2. Describe detector operation, including how the search is to be conducted and what procedures (including response) are followed in the event of an alarm. Identify the training an operator receives in conducting the search.
3. Identify any area characteristics, e.g., air contamination, that could lessen effective operation, and describe means used to compensate for such characteristics.
4. Describe redundant physical protection components or procedures that can be used to perform this function in the event of detector failure.
5. Describe the frequency and kind of preventive maintenance and operational testing.
- \*6. Identify by personnel category all facility employees and others who have access past this safeguard.

- \*7. Identify by personnel category all facility employees and others who have control of this safeguard.

34. EXPLOSIVE DETECTOR  
- Hand-Held, Vehicle Search

1. Describe the type of detector, where it is used, and its performance specifications in terms of type and quantity of material that can be detected, probability of detection, and false alarm rate.
  2. Describe detector operation, including how the search is to be conducted and what procedures (including response) are followed in the event of an alarm.
  3. Identify any area characteristics, e.g., air contamination, that could lessen effective operation, and describe means used to compensate for such characteristics.
  4. Describe redundant physical protection components or procedures that can be used to perform this function in the event of detector failure.
  5. Describe the frequency and kind of preventive maintenance and operational testing.
- \*6. Identify by personnel category all facility employees and others who have access past this safeguard.
- \*7. Identify by personnel category all facility employees and others who have control of this safeguard.

35. EXPLOSIVE DETECTOR  
- Volume

1. Describe the type of detector, its location, and its performance specifications in terms of type and quantity of material that can be detected, probability of detection, and false alarm rate.
2. Describe detector operation, including how the search is to be conducted and what procedures (including response) are followed in the event of an alarm.
3. Describe the installation, including augmenting components such as closed circuit television (CCTV) or audio links. If the installation differs from manufacturer's recommendations, specify how and why.
4. Identify area characteristics, e.g., air contamination, that could lessen effective operation, and describe means used to compensate for such characteristics.

5. Describe redundant physical protection components or procedures that can be used to perform this function in the event of detector failure.
6. Describe the type and duration of backup power available.
7. Describe the frequency and kind of preventive maintenance and operational testing.
- \*8. Identify by personnel category all facility employees and others who have access past this safeguard.
- \*9. Identify by personnel category all facility employees and others who have control of this safeguard.

### 36. EXPLOSIVE DETECTOR - Walk-Through

1. Describe the type of detector, its location, and its performance specifications in terms of type and quantity of material that can be detected, probability of detection, and false alarm rate.
2. Describe detector operation, including how the search is to be conducted and what procedures (including response) are followed in the event of an alarm.
3. Describe the installation, including augmenting components such as CCTV or audio links. If the installation differs from manufacturer's recommendations, specify how and why.
4. Identify area characteristics, e.g., air contamination, that could lessen effective operation, and describe means used to compensate for such characteristics.
5. Describe redundant physical protection components or procedures that can be used to perform this function in the event of detector failure.
6. Describe the type and duration of backup power available.
7. Describe the frequency and kind of preventive maintenance and operational testing.
- \*8. Identify by personnel category all facility employees and others who have access past this safeguard.
- \*9. Identify by personnel category all facility employees and others who have control of this safeguard.

### 37. FENCE SYSTEMS

1. Describe the type of fence used and its intended purpose. Describe the area defined by the fence barrier, and indicate the relationship between the fence and the total perimeter system.

2. Describe the installation, addressing such factors as type and number of fence barriers installed, distance between fences, obstacles between fences, gauge of wire, size of mesh, height, top configuration, how the bottom is anchored, post size and spacing, and how the posts are anchored. State the penetration time for a single fence and the penetration time for all fences and obstacles.
3. Indicate the other physical protection components and measures (including personnel functions) used to monitor or provide backup security for the fence system. This should include a description of the fence lighting system.
4. Describe the known vulnerabilities of the fence and how they will be compensated for. This should include environmental conditions that tend to decrease penetration time or interfere with detection or assessment.

### 38. FLOORS, ROOFS, AND WALLS

1. Describe the type of floor, roof, or wall used. Indicate the area where it is located (PA, MAA, or VA), and specify its penetration delay time. (Calculations of penetration delay time are discussed in the Sandia Barrier Handbook.)
2. Describe what the floor, roof, or wall protects, and compare the floor, roof, or wall protection performance with surrounding or connected components.
3. Indicate other physical protection components and measures (including personnel functions) used to monitor or provide backup security for floors, roofs, or walls.
4. Describe the known vulnerabilities of the floors, roofs, or walls and how they are compensated for.

### 39. FUNCTIONAL ZONING

1. Describe what the functional zoning is expected to achieve, indicating how and where it will be used.
2. List the personnel, by function, who are required to conform to the functional zoning. Describe how duties are divided and allotted, and indicate whether duties are rotated among different groups. Indicate who is responsible for assigning duties.
3. Describe the training that personnel receive in participating in functional zoning.
4. Identify verification or audit methods that ensure functional zoning is properly executed.
5. Provide a descriptive outline of how functional zoning is used throughout the facility, indicating personnel procedures and number of zones encountered along potential paths from SNM to the PA perimeter.

6. Provide details on any other component(s) employed to minimize collusion and supplement functional zoning.

#### 40. GATES AND ASSOCIATED HARDWARE

1. Describe the location of the gate and how it will be used. List type and construction of the gate, along with its penetration time compared with surrounding fencing and hardware. Describe the installation and operation of the gate and its associated hardware.
2. Describe the area to which the gate controls access. Indicate what functions are performed in the areas adjacent to the gate.
3. Indicate the physical protection components and measures (including personnel functions) used to monitor or provide backup security for this component. These could include barriers, alarms, use of redundant gates, or guard patrol.
4. Describe the known vulnerabilities of the gates and how they will be compensated for.
- \*5. Identify by personnel category all facility employees and others who have access past this safeguard.
- \*6. Identify by personnel category all facility employees and others who have control of this safeguard.

#### 41. GUARD FORCE PERSONAL EQUIPMENT

1. List the personal equipment available to members of the guard force at the facility. Indicate whether the equipment is carried with the guard at all times or is stored. If stored, indicate location and preventive means to deter unauthorized use.
2. Indicate who has distributional control over the equipment. Describe any limitation on the distribution of the equipment within the guard force.
3. Briefly describe the training the guard force receives in the use of personal equipment.
4. Describe the procedures and methods used to maintain proper operability and availability of the equipment during both normal and emergency conditions.

#### 42. GUARD FORCE QUALIFICATIONS

1. Describe the level of performance expected from the guard force and the criteria used to determine qualifications.
2. Indicate how often security personnel will be requalified and how this requalification will be accomplished. List personnel, by function, with control over the guard force qualification program.

3. Identify monitoring methods that assess guard force ability to perform assigned tasks in a working environment.
4. Outline any discrepancies from the appropriate requirements of Appendix B to 10 CFR Part 73 with regard to guard force qualification.

#### 43. GUARD PATROLS AND INTERVENTION

1. Describe what guard patrols and intervention are expected to achieve. Indicate the areas within a facility where the patrols are conducted (use a map if necessary).
2. List all personnel, by function, who perform the patrols or intervention functions. Describe the manner in which patrol duty is assigned and the personnel responsible for the selection.
3. Indicate the training that personnel will receive in conducting a patrol, and identify the instructions received by the guards with respect to intruder intervention policy.
4. Identify verification or audit methods that ensure procedures are properly executed.
5. Outline how a guard patrol is performed. This should describe the different activities a patrol is expected to conduct, time required to complete a patrol, randomness of patrol, number of guards available for response, and average estimated response time per response route within the facility.
6. Describe any physical protection features designed to minimize collusion during patrols or intervention conditions.

#### 44. GUARD POST ASSIGNMENTS

1. List all personnel, by function, who are responsible for assigning guard posts and other personnel who will have advance knowledge of post assignment.
2. Identify the verification or audit methods that ensure assignments are properly executed.
3. Outline the procedures used to determine post assignments. Indicate how far in advance assignments are posted.
4. Describe the components employed to minimize collusion with regard to guard post assignment. This should include a description of the frequency of post rotation and randomness of rotation.
- \*5. Identify by personnel category all facility employees and others who have control of this safeguard.

#### 45. HARDWARE VIDEO SYSTEMS

1. Describe the type of video system, its location, and what it is intended to monitor.
2. Describe area characteristics that could lessen effective operation, and identify means used to minimize such characteristics.
3. Describe the installation. If the installation differs from manufacturer's recommendations, specify how and why.
4. Describe type and duration of backup power available.
5. Identify redundant equipment or procedures that can be used in the event of system failure.
6. Describe the frequency and kind of preventive maintenance and operational testing.
7. Describe tamper protection and line supervision used with the system.

#### 46. INFRARED BEAM SYSTEMS, EXTERIOR

1. Describe the type of system used, its location, and what it protects. Indicate its detection sensitivity. Describe reliability in terms of probability of detection and false alarm rate.
2. Describe area characteristics, either man made or environmental, that could lessen effective operations and measures used to compensate for such characteristics.
3. Describe the installation, including location of control or processing units. If the installation differs from manufacturer's recommendations, specify how and why.
4. Indicate where the alarm annunciates, how an alarm condition is assessed, and what response occurs when an alarm is indicated.
5. Describe type and duration of backup power available.
6. Identify any other physical protection system component or subsystem that provides direct redundant or backup protection in the event of alarm failure.
7. Describe tamper protection and line supervision used with the alarm.
8. Describe the frequency and kind of preventive maintenance and operational testing. Include any available data on mean time between failures.
- \*9. Identify by personnel category all facility employees and others who have access past this safeguard.

- \*10. Identify by personnel category all facility employees and others who have control of this safeguard.

47. INTERFACE BETWEEN ALARM STATION  
AND SENSORS

- Individual Hardwire Alarms
- Multiplexed Hardwire Alarms
- Hardwire Command Signals

1. Describe the type of interface, its location, and its function within alarm system operation.
2. Describe the operation of the interface, including how signals are processed.
3. Describe the installation. If the installation differs from manufacturer's recommendations, specify how and why.
4. Describe type and duration of backup power available.
5. Describe redundant equipment or procedures that can be used in the event of interface failure.
6. Describe the frequency and kind of preventive maintenance and operational testing.
7. Describe tamper protection and line supervision used with the system.

48. ISOLATION ZONES

1. Describe the purpose of the isolation zone, indicating its location within the facility with respect to PAs, MAAs, and VAs. Indicate the size of the zone, what the terrain will be like, and what will be done to restrict vegetation growth in the zones.
2. Indicate all physical protection components and measures (including personnel functions) used to monitor or provide backup security for this area. These could include security lighting, perimeter alarms, CCTV systems, or guard force patrols.
3. Describe the known vulnerabilities of the zone such as anticipated blind spots or problem areas within the zone and how they will be compensated for.

49. K-9s, USED FOR PACKAGE OR VEHICLE  
SEARCH

1. Indicate what the use of K-9s in package or vehicle searches is intended to achieve. Describe when and where it will be done and the material to be searched for. If vehicle search, describe what areas of the vehicle are searched.

2. List the K-9 handlers, by function, and indicate how they are chosen and who is responsible for selecting them.
3. Describe the training program that the animals and handlers have successfully completed. Indicate how often this training is updated and whether the animal and handler are recertified on a regular basis. Outline any other activities or procedures used to maintain the animals' sensitivity toward the object to be detected.
4. Identify any verification or audit methods that ensure that the search is properly executed.
5. Outline how the search is performed and the typical working shift of the K-9, stating length of working shift, how the handler might help the K-9 search, whether dogs are rotated among handlers, how thorough a search is made, and how much time is spent on a search.
6. Describe the conditions under which the search is conducted. Indicate how clear the areas will be kept of exhaust fumes, chemical odors, etc., and whether handlers will minimize the use of "scented" toiletry products that might contribute to "nuisance" alarms.
- \*7. Identify by personnel category all facility employees and others who have access past this safeguard.
- \*8. Identify by personnel category all facility employees and others who have control of this safeguard.

#### 50. LOCAL AUDIBLE OR VISIBLE ALARMS

1. Describe the type of alarm used, its location, and what it protects. Specify how it is to be used, indicator intensity, and sensitivity of the detector used with the alarm. Include reliability data in terms of probability of detection and false alarm rate.
2. Describe area characteristics, man made or environmental, that could lessen effective operation. Identify measures used to compensate for such characteristics.
3. Describe the installation, including location of control or processing units. If the installation differs from manufacturer's recommendations, specify how and why.
4. Indicate how the alarm is responded to and who is responsible for response and alarm reset.
5. Describe the type and duration of backup power available.
6. Identify any other physical protection system component or subsystem that provides direct redundant or backup protection in the event of system failure.

7. Describe tamper protection and line supervision used with the system.
8. Describe the frequency and kind of preventive maintenance and operational testing. Include any available data on mean time between failures.
- \*9. Identify by personnel category all facility employees and others who have access past this safeguard.
- \*10. Identify by personnel category all facility employees and others who have control of this safeguard.

#### 51. LOCKS (KEYED, KEYLESS)

1. Describe the type and location of all locks. Specify the standards that the locks will meet. Indicate the estimated penetration delay time of the locks.
2. Describe the area that the lock protects. Indicate the penetration delay time of surrounding components or hardware.
3. Identify any physical means used to minimize tampering or compromising of the lock. This could include hardened body guardplates or shields, shrouded shackle and bolts, equivalent melting points of key mechanism and surrounding mechanism, anti-pick or decoding features, or positively coupled locking mechanism. Indicate if the locks are corrosionproof. For electronic locks, describe their operation in the event of a power failure. This should include a description of emergency power available, whether a keylock override exists, and status of the lock in a nonenergized condition.
4. Describe any other known vulnerabilities of the lock not described in 3 above and indicate how they are compensated for.
5. Indicate who has control over the locks and the degree of master keying used throughout the facility. Describe when and how often the lock combinations will be changed. List the personnel, by function, who are involved in this decisionmaking and who perform maintenance.
- \*6. Identify by personnel category all facility employees and others who have access past this safeguard.
- \*7. Identify by personnel category all facility employees and others who have control of this safeguard.

#### 52. MANUAL ALARM RECORDING

1. Describe the function of manual alarm recording and the circumstances under which it will be used.
2. List all personnel, by function, responsible for manually recording alarms at the CAS and SAS. Indicate how they are chosen and the person(s) responsible for the assignment, verification, or review of this information.

3. Identify verification or audit methods that ensure the task is properly executed.
4. Outline how this task will be performed, describing the type of alarms to be manually recorded and the items of information that will be recorded in the log in response to an alarm. Include information on how soon after an alarm the information is recorded and for how long this information is stored.
- \*5. Identify by personnel category all facility employees and others who have access past this safeguard.
- \*6. Identify by personnel category all facility employees and others who have control of this safeguard.

### 53. MASTER (FIXED) RADIO

1. Describe the type of radio, its location, and how it will be used. Identify nominal channel capability, known channel interference, and modulation and power characteristics in terms of their ability to ensure reliable communications with local law enforcement and internal site locations.
2. Describe the installation, including antenna and transmission line location. Describe any environmental characteristics that could adversely affect performance, location of "dead spots" within the facility, and methods employed to counter interference.
3. Describe the type and duration of backup power.
4. Identify any redundant communication capability.
5. Describe the frequency and kind of preventive maintenance and operational testing.

### 54. MICROWAVE SYSTEMS, EXTERIOR

1. Describe the type of microwave system used, its location, and what it protects. Indicate its detection sensitivity in terms of intruder size, speed, and mode of advancement and reliability in terms of probability of detection and false alarm rate.
2. Describe the area characteristics, either man made or environmental, that could lessen effective operation. Identify measures used to compensate for such characteristics.
3. Describe the installation, including location of control or processing units. If the installation differs from manufacturer's recommendations, specify how and why.
4. Indicate where the alarm annunciates, how an alarm condition is assessed, and what response occurs when an alarm is initiated.

5. Describe the type and duration of backup power available.
6. Identify any other physical protection system component or subsystem that provides direct redundant or backup protection in the event of alarm failure.
7. Describe tamper protection and line supervision used with the alarm.
8. Describe the frequency and kind of preventive maintenance and operational testing. Include any available data on mean time between failures.
- \*9. Identify by personnel category all facility employees and others who have access past this safeguard.
- \*10. Identify by personnel category all facility employees and others who have control of this safeguard.

#### 55. MOBILE RADIO

1. Describe the type of mobile radio used, what physical protection purpose the radio serves, and how it is used and by whom. Identify frequency, modulation, and power specifications in terms of how they ensure reliable communication.
2. Describe characteristics within the radio coverage area, e.g., dead spots, that could lessen effective operation. Identify measures used to compensate for such characteristics.
3. Identify any redundant communication capability available in the event of failure.
4. Describe the frequency and kind of preventive maintenance and operational testing.
5. Describe any means used to verify that transmissions are bona fide.
6. Describe backup power available.

#### 56. MOTION DETECTORS

- Interior Infrared Beam Systems
- Interior Microwave Systems
- Ultrasonic and Sonic Systems

1. Describe the type of system used, its location, and what it protects. Indicate its detection sensitivity in terms of intruder size, speed, and mode of advancement and reliability in terms of probability of detection and false alarm rate.
2. Describe area characteristics, either man made or environmental, that could lessen effective operation. Identify measures used to compensate for such characteristics.

3. Describe the installation, including location of control or processing units. If the installation differs from manufacturer's recommendations, specify how and why.
4. Indicate where the alarm annunciates, how an alarm condition is assessed, and what response occurs when an alarm is indicated.
5. Describe the type and duration of backup power available.
6. Identify any other physical protection system component or subsystem that provides direct redundant or backup protection in the event of alarm failure.
7. Describe tamper protection and line supervision used with the alarm.
8. Describe the frequency and kind of preventive maintenance and operational testing. Include any available data on mean time between failures.
- \*9. Identify by personnel category all facility employees and others who have access past this safeguard.
- \*10. Identify by personnel category all facility employees and others who have control of this safeguard.

#### 57. MULTI-MAN RULE

1. Describe what multi-man rule procedures are expected to achieve, indicating when, where, and under what circumstances the procedures will be followed.
2. List all personnel, by function, who may participate in multi-man teams. Explain how teams are formed and areas assigned. Identify, by function, the personnel responsible for assigning teams and areas.
3. Describe the instructions that personnel will receive in meeting the multi-man rule requirements.
4. Identify verification or audit methods that ensure the multi-man rule is properly executed.
5. Outline how the multi-man rule procedure is performed.
6. Describe the methods used to minimize collusion among personnel involved with multi-man rule procedures. This should include the degree to which teams are randomly rotated, how long in advance teams and areas are assigned, and who has knowledge of specific assignments.
- \*7. Identify by personnel category all facility employees and others who have control of this safeguard.

#### 58. NIGHT VISION DEVICES

1. Describe the type of night vision device (NVD) that will be used and the function it will perform. Indicate the criteria used to select the device

and measures taken to ensure it is properly suited for its planned environment. Specify the device's capabilities and sensitivities, and identify the conditions under which it will be used.

2. List all personnel, by function, who will have access to the NVD, including individuals who perform maintenance and testing of the device.
3. Describe the training users will receive in proper operation of the device.
4. Describe the planned testing and maintenance program for the NVD, indicating frequency of equipment operability checks.
5. Identify audit and control methods that ensure authorized use of the NVD.
6. Identify other equipment that will be used in conjunction with the NVD. Describe the availability of the NVD to its users, and indicate all locations where the device is normally stored.

#### 59. PAT-DOWN SEARCH

1. Describe what a pat-down search is expected to accomplish, indicating when and where it will be used.
2. List, by function, the personnel who perform the search, and indicate how they are selected for this task and the personnel responsible for the selection.
3. Describe the training received by personnel in performing the search.
4. Describe the verification or audit methods that ensure that the search is properly executed.
5. Outline how the pat-down search is performed. This should include such information as parts of the body and clothing that will be searched, time spent on the search, whether the searcher will be armed, whether guards of either sex will be available to conduct searches, and restrictions on type of clothing and articles personnel may wear or carry while being searched.
6. Describe the methods used to deter collusion among personnel who are involved in the search.
- \*7. Identify by personnel category all facility employees and others who have access past this safeguard.
- \*8. Identify by personnel category all facility employees and others who have control of this safeguard.

## 60. PERSONAL IDENTIFICATION NUMBERS AND PASSWORDS

1. Describe the function of the personal identification (ID) numbers and passwords, indicating how, when, and where they are used.
2. List the personnel, by function, who use these numbers and passwords for identification and verification. Indicate personnel, by function, who perform the verification, how these personnel are chosen, and personnel responsible for the assignment of verification duties. Indicate personnel, by function, with access to the numbers and passwords.
3. Describe the instructions personnel will receive in the use of personal ID numbers and passwords.
4. Identify verification or control methods that ensure these numbers and passwords are properly used.
5. Outline how the personal ID numbers and passwords are used. Include information on how the numbers and passwords are generated and the areas to which the personal ID numbers and passwords grant access.
6. Describe any methods used to prevent collusion among personnel who use the personal ID numbers or passwords. This would include a description of the circumstances that dictate number and password changes and frequency of changes.

## 61. PHOTO IDENTIFICATION BADGES

1. Identify the purpose of the photo ID badge system. Indicate the areas where the system will be used and the personnel to whom badges will be issued. Describe the ID badge, addressing such factors as badge material, degree of difficulty involved in counterfeiting the badge, number of badges issued, and frequency of photo update.
2. Identify the personnel, by function, responsible for distribution and production of the badges. Identify personnel, by function, with access to blank badges.
3. Describe the training the guard force will receive in implementing the photo ID badge system. A description of how facial comparisons will be made, what articles such as hats and sunglasses the individuals will be asked to remove, and amount of time spent on facial comparison should be included. Indicate any training that guards receive in facial feature recognition or facial comparison.
4. Identify verification or audit methods that ensure that the badge system is properly executed. List measures taken to ensure that other assigned duties do not interfere with the comparison process. If a remote comparison is made, describe the system used, indicating method of comparison and quality of transmitted image. Describe the testing of the photo ID badge system, indicating if testing is ever accomplished using "false" badges.

5. Indicate other physical protection components and measures, including personnel functions, used to monitor or provide backup security for this component. This should include a description of the security provided for blank badges.
6. Describe the methods used to deter collusion among personnel involved with the photo ID badge system.

#### 62. PHYSICAL CONTROLS AND PROCEDURES FOR KEYS, LOCKS, COMBINATIONS, AND CIPHER SYSTEMS

1. Describe what these controls and procedures are expected to achieve and where and how they will be used.
2. List all personnel, by function, who perform the controls and procedures, describing how these personnel are selected and the person(s) responsible for the selection.
3. Describe the instruction that personnel will receive in performing the procedures.
4. Identify the verification or audit methods that ensure that the physical controls and procedures are properly implemented or executed.
5. Outline the physical controls and procedures specifying when keys, locks, combinations, and cipher systems will be changed.
6. Describe the methods used to deter collusion among personnel who are involved with the physical controls and procedures for keys, locks, combinations, and cipher systems.

#### 63. PORTABLE RADIO

1. Describe the type of portable radio used, what safeguards purpose the radio serves, how it is used, and who operates it. Identify frequency, modulation, and power specifications in terms of how they ensure reliable communication.
2. Describe characteristics within the radio coverage area, e.g., dead spots that could lessen effective operation. Identify measures used to compensate for such characteristics.
3. Identify any redundant communication capability available in the event of failure.
4. Describe the frequency and kind of preventive maintenance and operational testing.
5. Describe any means used to verify that transmissions are bona fide.
6. Describe backup power available.

64. POSITIVE PERSONNEL IDENTITY  
VERIFICATION

- Fingerprints
- Handwriting
- Hand Geometry
- Voice Prints

1. Describe the type of system, its location, and its purpose within the physical protection system (e.g., identity verification, access control to VA). Indicate performance in terms of false acceptance and rejection rates.
2. Describe operation, including procedures followed in response to rejections.
3. Describe the installation, including tamper protection features.
4. Describe redundant physical protection equipment or procedures that can be used to perform this function in the event of system failure.
5. Describe the frequency and kind of preventive maintenance and operational testing.
6. Describe the characteristics and features of the personnel identification reference file, including tamper protection features.

65. RESPONSE VEHICLES

1. Describe the type of vehicle that will be used for response, indicating the number of vehicles available and where and how they will be located and used during a 24-hour period.
2. List the personnel, by function, who have access to the vehicle. Describe the function they perform with respect to the vehicle, and indicate any training or qualifications required of the personnel to perform the function. Identify how personnel are chosen to perform functions and who is responsible for the selection.
3. Describe the planned maintenance program for the response vehicle. Indicate how often preventive maintenance will be performed and what procedures will be followed in performing the maintenance. Describe the provisions made to ensure availability of a response vehicle under adverse conditions such as severe weather conditions or vehicle failure.
4. Describe the procedures or equipment used to prevent unauthorized use of vehicle.
5. Describe the known or anticipated vulnerabilities of the response vehicles and how they will be compensated for. The provisions made to ensure availability of a response vehicle under adverse conditions such as severe weather conditions or vehicle failure and the procedures or equipment used to prevent unauthorized use of the vehicle should be identified.

## 66. SALLY PORTS, PEDESTRIAN

1. Describe the type of sally port that will be used. Indicate the location of all pedestrian sally ports, using a map if necessary. Discuss the operation and structure of the sally port, including construction, penetration delay time of gates and adjacent fences, and conditions under which the sally port will be used.
2. Describe the area to which the sally port controls access.
3. Indicate the physical protection components and measures (including personnel functions) used to monitor or provide backup security for the sally port. Identify when and by whom the sally port will be monitored.
4. Identify the degree to which the sally port will be susceptible to external attack. Indicate the location of locking device protection afforded security personnel, the operability of gates if facility personnel should be disabled, and the alarm and communication systems used.
- \*5. Identify by personnel category all facility employees and others who have access past this safeguard.
- \*6. Identify by personnel category all facility employees and others who have control of this safeguard.

## 67. SALLY PORTS, VEHICLE

1. Describe the type of sally port that will be used. Indicate the location of all vehicle sally ports, using a map if necessary. Discuss the operation and structure of the sally port, including construction, penetration delay time of gates and adjacent fences, and conditions under which the sally port will be used.
2. Describe the area to which the sally port controls access.
3. Indicate the physical protection components and measures (including personnel functions) used to monitor or provide backup security for the sally port. Identify when and by whom the sally port will be monitored.
4. Identify the degree to which the sally port will be susceptible to external attack. Indicate the location of locking device protection afforded security personnel, the operability of gates if facility personnel should be disabled, and the alarm and communication systems used.
- \*5. Identify by personnel category all facility employees and others who have access past this safeguard.
- \*6. Identify by personnel category all facility employees and others who have control of this safeguard.

68. SHIELDING DETECTORS  
- Volume

1. Describe the type of detector, its location, and how it will be used. Indicate its detection sensitivity in terms of size and kind of material that can be detected and its reliability in terms of confidence level, probability of detection, and false alarm rate.
2. Describe operating procedures and requirements, including provisions to minimize false alarms, identification of operators and their training, minimum screening time required, and whether or not personnel are screened one at a time. Describe all mechanical or electronic systems or devices in or near the volume that could interfere with detector operation. Specify measures taken to minimize such interference.
3. Describe the installation, including location of controls. If the installation differs from manufacturer's recommendations, specify how and why.
4. Describe procedures used in the event of an alarm, including the response if shielding material is found.
5. Describe redundant or backup equipment or procedures to be used in the event of detector failure.
6. Describe the frequency and kind of preventive maintenance and operational testing.
- \*7. Identify by personnel category all facility employees and others who have access past this safeguard.
- \*8. Identify by personnel category all facility employees and others who have control of this safeguard.

69. SHIELDING DETECTORS  
- Walk-Through

1. Describe the type of detector, its location, and how it will be used. Indicate its detection sensitivity in terms of size and kind of material that can be detected and its reliability in terms of probability of detection, confidence level, and false alarm rate.
2. Describe operating procedures and requirements, including provisions to minimize false alarms, screening time required, etc.
3. Describe area characteristics that could lessen effective operation and means used to compensate for such characteristics.
4. Describe the installation. If the installation differs from manufacturer's recommendations, specify how and why.
5. Describe procedures used in the event of an alarm, including the response in the event shielding material is found. Describe the training an operator receives in conducting the search.

6. Describe redundant equipment or procedures used to perform this function in the event of detector failure.
7. Describe the frequency and kind of preventive maintenance and operational testing.
- \*8. Identify by personnel category all facility employees and others who have access past this safeguard.
- \*9. Identify by personnel category all facility employees and others who have control of this safeguard.

#### 70. SNM CONTAINERS

1. Describe how and where the SNM container is used. Describe the container itself, specifying size, penetration resistance (i.e., delay time), and identification or labeling for both in-process and storage conditions.
2. Indicate the physical protection components and measures (including personnel functions) used to monitor or provide additional security for this component. Describe the SNM container recordkeeping procedures, and indicate if records are kept for quantity of SNM in each container, location of containers, disposition of containers, and container tamper-sealing devices.
3. Describe the known or anticipated vulnerabilities of the container and how they will be compensated for.

#### 71. SNM DETECTORS

##### - Hand-Held, Package Search

1. Describe the type of detector and where it is used, and specify performance in terms of probability of detection and false alarm rate, given a specified test sample.
2. Describe operation, including search procedures and response procedures. Include the percentage of packages searched, how they are searched, and what actions are taken in the event of an alarm. Describe area characteristics that could interfere with effective operation and the means used to compensate for such characteristics.
3. Describe redundant or backup equipment or procedures to be used in the event of detector failure.
4. Describe the frequency and kind of preventive maintenance and operational testing, including calibration and testing criteria used.
- \*5. Identify by personnel category all facility employees and others who have access past this safeguard.
- \*6. Identify by personnel category all facility employees and others who have control of this safeguard.

72. SNM DETECTORS  
- Hand-Held, Personnel Search

1. Describe the type of detector and where it is used, and specify performance in terms of probability of detection and false alarm rate, given a specified test sample.
2. Describe operation, including search and response procedures. Specify how personnel are selected for search and how the search is conducted.
3. Describe area characteristics that could interfere with effective operation and the means used to compensate for such characteristics.
4. Describe redundant or backup equipment or procedures to be used in the event of detector failure.
5. Describe the frequency and kind of preventive maintenance and operational testing, including calibration and testing criteria used.
- \*6. Identify by personnel category all facility employees and others who have access past this safeguard.
- \*7. Identify by personnel category all facility employees and others who have control of this safeguard.

73. SNM DETECTORS  
- Volume

1. Describe the type of detector and its location, and specify performance in terms of probability of detection and false alarm rate, given a specified test sample.
2. Describe operation, including search and response procedures.
3. Describe the installation, including how and where the presence of SNM is annunciated. Describe any area characteristics that could interfere with effective operation and the means used to compensate for such characteristics.
4. Describe redundant or backup equipment or procedures to be used in the event of detector failure.
5. Describe duration and type of backup power available.
6. Describe the frequency and kind of preventive maintenance, and operational testing, including calibration and testing criteria used.
- \*7. Identify by personnel category all facility employees and others who have access past this safeguard.
- \*8. Identify by personnel category all facility employees and others who have control of this safeguard.

74. SNM DETECTORS  
-Walk-Through

1. Describe the type of detector and its location, and specify performance in terms of probability of detection and false alarm rate, given a specified test sample.
2. Describe operation, including search and response procedures.
3. Describe the installation, including how and where the presence of SNM is annunciated. Describe any area characteristics that could interfere with effective operation and the means used to compensate for such characteristics.
4. Describe redundant or backup equipment or procedures to be used in the event of detector failure.
5. Describe duration and type of backup power available.
6. Describe the frequency and kind of preventive maintenance and operational testing, including calibration and testing criteria used.
- \*7. Identify by personnel category all facility employees and others who have access past this safeguard.
- \*8. Identify by personnel category all facility employees and others who have control of this safeguard.

75. SNM HOLDING/STORAGE AREAS

1. Describe the function of the SNM holding/storage areas, and indicate under what conditions they are used to store or hold SNM. Describe the location of these areas for the MAA and PA of the facility. Indicate separation distances between barriers, number of barriers, and size of isolation zones. Specify their penetration delay time. (Calculations of penetration delay time are discussed in the Sandia Barrier Handbook.)
2. Identify the quantity of material that will typically be held or stored in these areas. Describe the areas contiguous to SNM holding/storage areas.
3. Indicate the physical protection components and measures (including personnel functions) used to monitor or provide backup security for these areas. Describe the type of container used.
4. Describe the material control and accounting procedures followed for SNM holding/storage areas. Indicate substantiating measurement methods for identity and quantity and also updating procedures to determine current status of the SNM.
5. Describe the known vulnerabilities of the holding/storage areas and how they are compensated for.

#### 76. SNM IDENTIFICATION/AUTHORIZATION PROCEDURES

1. Describe what SNM identification/authorization procedures are expected to achieve and where and how they will be used.
2. List all personnel, by function, who perform SNM identification and authorization, describing how these personnel are selected and the person(s) responsible for the selection.
3. Describe the training that personnel will receive in performing SNM identification/authorization procedures.
4. Identify the verification or audit methods that ensure that SNM identification/authorization procedures are properly executed.
5. Outline SNM identification/authorization procedures.
6. Describe methods used to deter collusion among personnel who perform SNM identification/authorization.

#### 77. SNM LIQUID AND SOLID WASTE HANDLING PROCEDURES

1. Describe what these handling procedures are expected to accomplish and where and how they will be used. Describe other activities conducted in the area.
2. List all personnel, by function, who perform the procedures, describing how these personnel are selected and the person(s) responsible for the selection.
3. Describe the instructions that personnel will receive in performing the procedures.
4. Identify the verification or audit methods that ensure that SNM liquid and solid waste handling procedures are properly executed.
5. Outline SNM liquid and solid waste handling procedures, including the procedures used when an assay of a waste package indicates a higher than acceptable quantity of SNM or when a security check indicates a waste package has been tampered with.
6. Describe methods used to deter collusion among personnel who perform SNM liquid and solid waste handling procedures.
7. Describe the containers used to hold the waste.

#### 78. SNM SCRAP REMOVAL PROCEDURES

1. Describe what the SNM scrap removal procedures are expected to achieve, indicating where and how they will be used and any other activities conducted in the area.

2. List all personnel, by function, who perform SNM scrap removal, describing how these personnel are selected and the person(s) responsible for the selection.
3. Describe the instructions that personnel will receive in performing the procedures.
4. Identify the verification or audit methods that ensure that the procedures are properly executed.
5. Outline SNM scrap removal procedures, including such items as packaging methods, SNM segregation categories, and procedures followed when an assay of the scrap indicates a higher than acceptable quantity of SNM.
6. Describe methods used to deter collusion among personnel who perform equipment checks and maintenance.

#### 79. SNM SHIPPING AND RECEIVING PROCEDURES

1. Describe what SNM shipping and receiving procedures are expected to achieve. Indicate where and how the procedures will be used.
2. List all personnel, by function, who perform the SNM shipping and receiving procedures, describing how these personnel are selected and the person(s) responsible for the selection.
3. Describe the instructions that personnel will receive in performing the SNM shipping and receiving.
4. Identify the verification or audit methods that ensure that SNM shipping and receiving is properly executed. Such items as carrier identity verification, tamper-seal control and inventory program, and recordkeeping procedures should be included.
5. Outline SNM shipping and receiving procedures.
6. Describe methods used to deter collusion among personnel who perform SNM shipping and receiving.
7. Identify the means of surveillance for the SNM while in transit, and describe whether the surveillance is continuous or not.

#### 80. TAMPER-INDICATING CIRCUITRY

1. Describe the type of tamper-indicating circuitry, with what equipment it is used, and how it operates (e.g., switch activates when cover plate is removed, or 20 percent circuit current change activates alarm).
2. Indicate where the alarm annunciates, how an alarm condition is assessed, and what response occurs when an alarm is indicated.
3. Describe the type and duration of backup power available.

## 81. TAMPER-INDICATING SEALS AND TAMPER-SEAL INSPECTION

1. Describe the function of the tamper-seal inspection. Describe the type of tamper seal used, indicating how it is applied and how it is designed to indicate tampering. Identify all situations where tamper-indicating seals are used.
2. List all personnel, by function, who are involved with tamper-seal inspection and accounting procedures. Indicate how inspectors are chosen and the personnel responsible for the selection.
3. Identify verification or audit methods that ensure procedures are properly executed. A description of the inventory methods used to account for the seals, provisions taken to prevent unauthorized use or procurement of seals, and destruction methods employed before an authorized entry should be included.
4. Outline the procedures used to inspect the seals. Include such information as frequency of seal inspection and the steps taken during an inspection when a seal is found to be damaged, broken, missing, improperly applied, or is found to have a serial number discrepancy.
5. Describe methods used to deter collusion among seal inspectors or personnel involved in seal auditing.

## 82. TEAM ZONING

1. Describe what the procedures of team zoning are expected to accomplish. Indicate how and where it will be used. Include a map, if necessary.
2. List all personnel, by function, who comprise the team, describing how these personnel are selected and the persons responsible for the selection. Indicate whether rotation among teams exists.
3. Describe the instructions that personnel will receive in properly performing the procedure.
4. Identify verification or audit methods that ensure that team zoning is properly executed.
5. Outline how team zoning is performed.
6. Describe methods used to deter collusion among personnel who comprise the team.

## 83. UNINTERRUPTIBLE POWER SYSTEMS

1. Describe the function of the uninterruptible power system (UPS), including location, what equipment it supplies, and length of time it can supply the required load.

2. List the personnel, by function, with control over the UPS, indicating personnel who perform testing and maintenance.
3. Specify the testing and maintenance procedures of the UPS. Describe how often the system will be functionally tested and how system security will be provided at all times, including during maintenance periods. Indicate whether maintenance will be "as needed," preventive, or both.
4. Describe the performance of the UPS when commercial power is lost.
5. Indicate what type of security is provided for the UPS, and describe any detrimental environmental conditions to which it may be exposed.
6. Indicate other physical protection components and measures, including personnel functions, used to monitor or provide security for the UPS.
7. Describe known vulnerabilities such as detrimental environmental conditions to which the UPS will be exposed and how they will be compensated for.

#### 84. VAULTS

1. State the purpose of the vault. Identify the vault location within the building structure, within the MAA, and within the PA. Also indicate the vault location with respect to the points where alarm assessments are to be made and response forces dispatched. Refer to maps and drawings as necessary.
2. Indicate the type and quantity of material stored in the vault and how the material is stored, e.g., type of container used.
3. Describe the construction of the vault, addressing such factors as walls, floor, roof, security lighting, air and utility passages, conduit and cable runs, doors, and locking hardware. State the expected penetration time with full consideration given to all components that make up the vault and the tools the adversary would be expected to use in making the penetration.
4. Indicate the physical protection components and measures (including personnel functions) used to monitor or provide backup security for the component. Describe the alarm system that will be used, indicating the location of the sensors, processors, and alarm cabling. Describe the assessment method to be used, and indicate the location of CCTV cameras and monitors (if used), where the assessment is to be made and by whom, the number of personnel who will respond to an alarm condition, and the expected response time. Indicate the degree to which the exterior surfaces of the vault are accessible for visual inspection, surveillance, and assessment.
5. Estimate the frequency of access to the vault. Describe the entry control procedures to be followed when entering the vault. Address such factors as person(s) who can authorize entry, person(s) who control the keys and combinations, procedures for placing the alarms into the access mode, procedures for verifying the integrity of seals (if used), person(s) authorized to enter the vault, and person(s) authorized to remove material from the

vault. Describe the means by which entry authority is authenticated and the methods used to verify identities.

6. Describe the known or anticipated vulnerabilities of the vault and how they will be compensated for.
- \*7. Identify by personnel category all facility employees and others who have access past this safeguard.
- \*8. Identify by personnel category all facility employees and others who have control of this safeguard.

#### 85. VIBRATION SENSORS

1. Describe the type of vibration sensor, its location, and what it protects. Specify its detection sensitivity and reliability in terms of probability of detection and false alarm rate.
2. Describe area characteristics, man made or environmental, that could lessen effective operation. Identify measures used to compensate for such characteristics.
3. Describe the installation, including location of control or processing units. If the installation differs from manufacturer's recommendations, specify how and why.
4. Indicate where the alarm annunciates, how an alarm is assessed, and what response occurs when an alarm is indicated.
5. Describe the type and duration of backup power available.
6. Identify any other physical protection system component or subsystem that provides direct redundant or backup protection in the event of alarm failure.
7. Describe tamper protection and line supervision used with the alarm.
8. Describe the frequency and kind of preventive maintenance and operational testing. Include any available data on mean time between failures.
- \*9. Identify by personnel category all facility employees and others who have access past this safeguard.
- \*10. Identify by personnel category all facility employees and others who have control of this safeguard.

#### 86. VISUAL INSPECTION, PACKAGE SEARCH

1. Describe what the search is expected to accomplish, indicating what is being searched for and when and where the search will be performed.
2. List, by function, the personnel who perform the search, and describe how they are selected and the personnel responsible for the selection.

3. Describe the training received by guard personnel to perform the inspection, indicating the amount of formal training and whether the training includes explosive, incendiary, or weapon recognition.
4. Identify verification or audit methods that ensure the search is properly executed.
5. Outline how the inspection is performed, indicating how it is determined which packages will be searched, how much time will be spent on a search, and how thoroughly a package is searched.
6. Describe the methods used to deter collusion among personnel who are involved in the search.
- \*7. Identify by personnel category all facility employees and others who have access past this safeguard.
- \*8. Identify by personnel category all facility employees and others who have control of this safeguard.

#### 87. VISUAL INSPECTION, VEHICLE SEARCH

1. Describe what the vehicle search by visual inspection is expected to accomplish, indicating what will be searched for and when and where the search will be conducted.
2. List, by function, the personnel who perform the search. Describe how they are selected and the personnel responsible for the selection.
3. Describe the level of training provided the search team members with respect to the areas of the vehicle to search, identification of contraband items, and procedures to follow if contraband is found.
4. Identify verification or audit methods that ensure procedures are properly executed.
5. Outline how the search is performed. Address such factors as time allotted for inspection, equipment available to aid in the search, and whether cargo will be subject to a separate search.
6. Describe the methods used to deter collusion among personnel who are involved in the search.
- \*7. Identify by personnel category all facility employees and others who have access past this safeguard.
- \*8. Identify by personnel category all facility employees and others who have control of this safeguard.

88. WEAPONS

- Handgun
- Semiautomatic
- Shotgun

1. Describe the weapons available to the guard force at the facility, indicating type, number, where stored, availability of ammunition, and quantity of ammunition issued upon weapon distribution.
2. Identify all personnel with access to the weapons, and identify who has control over their distribution during emergency conditions.
3. Indicate how often preventive maintenance is performed on the weapons to ensure proper operation in emergency conditions.
4. Outline the training that personnel receive in the proper use of the weapons, and indicate the function of all those who receive the training.
5. If a weapon is stored, describe what measures will be taken to prevent its unauthorized use.

89. WEAPONS DETECTOR

- Hand-Held, Package and Personnel Search

1. Describe the type of detector and where it is used, and specify performance in terms of probability of detection and false alarm rate, given a specified test sample.
2. Describe the search operation, including procedures used in response to an alarm.
3. Describe redundant or backup equipment or procedures that can be used in the event of detector failure.
4. Describe the frequency and kind of preventive maintenance and operational testing.
- \*5. Identify by personnel category all facility employees and others who have access past this safeguard.
- \*6. Identify by personnel category all facility employees and others who have control of this safeguard.

90. WEAPONS DETECTOR

- Volume

1. Describe the type of detector and its location, and specify performance in terms of probability of detection and false alarm rate, given a specified test sample.

2. Describe the operation of the weapons detector, including search and response procedures.
3. Describe the installation. If the installation differs from manufacturer's recommendations, specify how and why. Describe area characteristics that could interfere with effective operation and the means used to compensate for such characteristics.
4. Describe redundant or backup equipment or procedures that can be used in the event of detector failure.
5. Describe the duration and type of backup power available.
6. Describe the frequency and kind of preventive maintenance and operational testing.
- \*7. Identify by personnel category all facility employees and others who have access past this safeguard.
- \*8. Identify by personnel category all facility employees and others who have control of this safeguard.

91. WEAPONS DETECTOR  
- Walk-Through

1. Describe the type of detector and where it is located, and specify performance in terms of probability of detection and false alarm rate, given a specified test sample.
2. Describe operation, including search and response procedures used.
3. Describe the installation. If the installation differs from manufacturer's recommendations, specify how and why. Describe area characteristics that could interfere with effective operation and the means used to compensate for such characteristics.
4. Describe any redundant or backup equipment or procedures that can be used in the event of detector failure.
5. Describe the duration and type of backup power available.
6. Describe the frequency and kind of preventive maintenance and operational testing.
- \*7. Identify by personnel category all facility employees and others who have access past this safeguard.
- \*8. Identify by personnel category all facility employees and others who have control of this safeguard.

## 92. WINDOWS AND ASSOCIATED HARDWARE

1. Describe the type of window used, addressing such factors as size, type of glazing, whether it can be opened and, if so, the type of locking hardware and its installation. Identify the size of the window pane (if multipane) and the type of frame and how it is anchored. Describe protective grills, (if used) and how they are attached. Indicate the areas where it is located, and specify its penetration delay time. (Calculations of penetration delay time are discussed in the Sandia Barrier Handbook.)
2. If the window is part of a barrier intended to protect material or components, describe what it protects. Compare the window's protective performance with surrounding or connected components.
3. Indicate other physical protection components and measures, including personnel functions, used to monitor or provide backup security for the window.
4. Describe the known vulnerabilities of the window and how they are compensated for.

## 93. X-RAY PACKAGE AND CONTAINER SEARCH

1. Describe the type of system used, its location, and what material it is intended to detect. Specify performance in terms of sensitivity and discrimination, and identify the maximum package dimensions that can be handled.
2. Describe the search operation, including search and response procedures used.
3. Describe the installation. If the installation differs from manufacturer's recommendations, specify how and why. Describe area characteristics that could interfere with effective operation and the means used to compensate for such characteristics.
4. Describe redundant or backup equipment or procedures that can be used to conduct the search function in the event of detector failure.
5. Describe the duration and type of backup power available.
6. Describe the frequency and kind of preventive maintenance and operational testing.
- \*7. Identify by personnel category all facility employees and others who have access past this safeguard.
- \*8. Identify by personnel category all facility employees and others who have control of this safeguard.

## ATTACHMENT A

### SAMPLE PORTION OF PHYSICAL PROTECTION PLAN\*

This attachment contains a sample portion of a protection plan developed for a hypothetical facility. The portion presented corresponds with Chapter 18, "Prevent Unauthorized Access of Persons and Materials into Material Access Areas and Vital Areas," of this Standard Format. For clarity, the hypothetical facility does not contain a VA and hence discussion is limited to preventing unauthorized access to MAAs and vaults. (In an actual plan, VAs would receive discussion similar to that concerned with MAAs.) Located in Appendix 1 to this sample plan are example responses to some of the Information Request Sheets (IRSs) referenced in this sample plan. Inspection of the partial sample plan and IRSs will help the reader understand both the level of detail needed by the NRC and a format in which the information in the protection plan may be presented.

#### 18. PREVENT UNAUTHORIZED ACCESS OF PERSONS AND MATERIALS INTO MATERIAL ACCESS AREAS AND VITAL AREAS

This section describes the systems, subsystems, components, and procedures used to ensure that attempts by personnel to gain unauthorized access or to introduce unauthorized materials are detected, assessed, and communicated. All attempts, either by force, stealth, or deceit, result in a timely response initiated to deter, delay, or deny the unauthorized access or penetration. These entry controls satisfy the performance capability requirements of paragraph 73.45(b) of 10 CFR Part 73.

##### 18.1 Entry Control Through MAA and VA Entry Portals

Figure 18-1 identifies the MAA, the vault, and the associated portals. One entry/exit point (Ref. 21) penetrates the east wall, and one emergency exit (Ref. 28) penetrates the north wall of the MAA. One entry/exit point (Ref. 21) penetrates the south wall of the vault (Ref. 84).

##### 18.1.1 Entry Authorization Procedures

Entry authorization verification procedures (Ref. 2) limit MAA and vault admittance to only those personnel authorized to perform specifically assigned tasks and at only those times when the performance of these activities is authorized. Authorization Schedules (Ref. 1) determine what activities are authorized and when and by whom these activities are conducted. Entry procedures progressively become more restrictive as the sensitivity of the area being accessed increases.

Entry authorization consists of a computerized criteria screening process. This process compares area access criteria against personnel access qualifications (Table 18-1 and Refs. 1 and 2).

---

\*References included in Attachment A refer to those Information Request Sheets described from page 5.52-27 to page 5.52-72 of this guide.

Personnel entry authorization is initiated and verified each time an individual requests admittance to an MAA.

Personnel entry authorization is maintained current by continuously updating the Personnel Authorization File and the Area Authorization File.

Authorization information is displayed on computer terminals located in manned entry/exit control points and at the Central Alarm Station and the Secondary Alarm Station.

The alarm stations have the capability of displaying a list of all personnel currently occupying a controlled access area and a record of all entry and exit events that have occurred within the last 24 hours.

#### 18.1.2 Entry Procedures and Controls for Routine Conditions

The combined use of security officers and entry control systems and procedures for identification, authorization, and search functions will detect unauthorized persons, contraband, and unauthorized vehicles attempting to enter an MAA. These measures are applied during both routine (Table 18-2) and nonroutine conditions.

Table 18-3 identifies generic criteria that govern access functions during routine working and nonworking conditions, excluding nonroutine conditions identified in Section 18.1.3.

18.1.2.1 Procedures and Controls for Personnel Entry. Personnel entry controls and procedures are designed and operated to verify admittance authorization and personnel identification prior to allowing admittance into the MAA entry/exit control point (Ref. 66) and the MAA, respectively. All admittance search functions are conducted within the control point that is isolated from both the MAA and the PA. This facilitates containment of personnel by security officers if suspicious activities are observed within the control point.

Vault entries require use of the two-man rule, additional authorization, and identification but do not require additional search.

##### 1. Material Access Area Entry

A coded credential badge (Ref. 14) is used to verify authorization and allow access to the entry/exit control point. Proper authorization also keys the personnel identification video-stored image system for use by the control point security officer (Ref. 64). Entering the control point enrolls the individual on the Personnel Inventory System as being in the MAA.

After an individual is in the entry point, the security officer ensures that the entrance door is closed and proceeds to establish identification (Refs. 14 and 64 and Tables 18-1 and 18-7). Authorization information is displayed to the security officer on a computer terminal for verification. A contraband search using walk-through and hand-held metal detectors (Refs. 72, 89, and 91 and Table 18-4), explosives detectors (Ref. 33 and Table 18-5), and an SNM detector (Ref. 74 and Table 18-6) is then conducted. After the admittance procedures are completed, a second individual is allowed access to the control point.

When authorization, identification, and search procedures are completed on the second individual, the security officer signals the alarm stations to allow entrance to the MAA. Either alarm station operator then actuates one of two door strikes on the entrance to the MAA. The second strike is actuated by a credential proximity reader that must be keyed by two credentials before it will operate. The alarm station operators then verify that two individuals actually enter the MAA by CCTV monitor (Ref. 10).

Vault entry is initiated by two individuals actuating the vault proximity reader with their coded credentials. This action verifies access authorization and signals the alarm stations that vault admittance is requested. The alarm station operators actuate the vault control-point door after verifying by CCTV (Ref. 11) that only two individuals are gaining admittance. CCTV monitoring of vault entry is also conducted by the MAA entry/exit control-point security officer. The alarm station operators verify by CCTV that only the individuals who requested admittance are in the control point and open a second door that allows access to the vault. Verification that the first vault control-point door closed is provided to the alarm stations by balanced magnetic switch signals (Ref. 6).

## 2. Personnel Escort

Reference 31 describes the procedures and policies for escorting visitors within an MAA and a vault.

## 3. Response to Suspected Unauthorized Personnel

### a. MAA

Requesting admittance to an MAA's entry point with a Coded Credential Badge that has been issued to an individual not possessing MAA admittance authorization automatically alerts the CAS, the SAS, and the security officer inside the control point of the attempted entry. The response is in accordance with Chapter 23 of this plan.

During admittance operations, should identification of an individual be questioned, contraband detected, or the activities of the individual warrant suspicion, the security officer does not indicate his concern to the individual. Instead, the security officer continues and prolongs the admittance operation until response personnel arrive at the control point. The security officer reports this situation to the CAS and the SAS in accordance with Chapter 23 of this plan.

### b. Vault

Requesting admittance to the vault with a Coded Credential Badge that has been issued to an individual not possessing vault admittance authorization automatically alerts the CAS, the SAS, and the security officer inside the MAA control point of the attempted entry. The response is in accordance with Chapter 23 of this plan.

18.1.2.2 Procedures and Controls for Introduced Materials. (Refer to Section \_\_\_\_\_ of the Fundamental Nuclear Material Control Plan for complementary description.) Materials that are presented for admittance into MAAs

will be subjected to different admittance screening measures based on the type of materials and the specified area involved. In addition to the procedures listed below, materials that are to be introduced into vaults will be verified according to procedures described in Reference 84.

For introduction of SSNM, the security officer verifies the authorization, type, and quantity of the material in accordance with the admittance authorization and verification procedures described in Reference 2. This verification includes inspection of tamper seals and other tamper-proofing items. Authorization verification is accomplished through the use of the computer communications terminal located at the MAA entry-exit control point.

Individuals desiring to introduce materials other than SSNM into an MAA or vault are required to submit a Security Work Order (SWO) to the Security Supervisor prior to entry. The SWO is then entered into the computer communications central storage file. When the materials are presented for introduction, the security officer retrieves the inventory listing by inputting the computer communications terminal with the SWO identification number. The security officer then checks the inventory listing against the materials being introduced to ensure that only authorized materials are admitted.

Materials are searched for contraband using those measures identified in Tables 18-4 through 18-6. All boxes, parcels, and packages are opened and inspected for concealed, unauthorized materials while within the MAA control point. Instrumentation and other similar components are checked to verify that tamper seals are authentic and that they have not been violated (Ref. 81).

In the event material that is not authorized is presented for admittance to the MAA or the vault, the security officer does not indicate his concern to the individual. Instead, the security officer continues and prolongs the admittance operation until response personnel arrive at the control point. The security officer reports the situation to the CAS or the SAS in accordance with Chapter 23 of this plan.

18.1.2.3 Procedures and Controls for Introduction of Vehicles. Facility configuration makes vehicle entry to the MAA or the vault impossible under all credible conditions.

### 18.1.3 Entry Procedures and Controls for Nonroutine Conditions

Nonroutine conditions are composed of one or more categories of contingency incidents or various nonroutine production and environmental conditions. These incidents are identified in the Site Emergency Plan. During the initial stages of a nonroutine condition, the exact status within the MAAs may not be known. However, to cope with the nonroutine condition in a manner that satisfies both the physical protection and emergency planning performance objectives, a blending of both planning concepts is used. Table 18-7 identifies nonroutine conditions and associated Work Designation Codes.

The authenticity of a nonroutine condition is verified in accordance with the Contingency Plan and Procedures (Ref. 16). Verification of the condition is communicated to all Security personnel in accordance with Chapter 23 of this plan.

## 1. Nonroutine Entry Authorization

The need for nonroutine admittance to an MAA cannot be anticipated during the preparation of a Production Schedule. Consequently, the area authorization file (Ref. 1) is updated continuously and as necessitated by the occurrence of such activities.

Individuals assigned to the various emergency response teams have Emergency Work Designation Codes (Table 18-7) added to their personal access qualifications. When an emergency occurs and its authenticity is verified, Emergency Work Designation Codes of required emergency response teams are used to authorize access to applicable areas for appropriate response personnel.

Entry procedures and controls specified in paragraph 18.1.2.1 are applied to all personnel desiring access to the MAA or the vault, except personnel possessing an A1 (fire) and A2 (personnel injury) Emergency Work Designation Code (Table 18-7).

## 2. Entry/Exit Control-Point Operations

Personnel designated A-2 responding to a personnel injury individually request admittance to the MAA control point by passing their Coded Credential Badge (Ref. 14) in front of the proximity reader. The A2 Emergency Work Designation Code permits entry, as specified in paragraph 18.1.2.1. The security officer ensures that only one individual enters the MAA control point at a time during admittance functions but does not conduct the contraband search. Personnel identification is established in accordance with paragraph 18.1.2.1. Entry to the vault is as specified in paragraph 18.1.2.1.

The nature of a fire, coupled with the potential malfunction of entry control components and the necessity for a personnel evacuation, places an extreme burden on personnel entry controls. Whenever possible, the MAA control point is used to assemble personnel responding to an A1 emergency. Should the fire make MAA control point occupancy impossible or degrade the performance capabilities of entry control components or procedures, the Protected Area (PA) control point is used as a focal point for consolidating fire response activities.

Personnel designated A1 responding to the fire individually request admittance to the MAA control point by passing their Coded Credential Badge (Ref. 14) in front of the proximity reader. The A1 Emergency Work Designation Code permits entry, as specified in paragraph 18.1.2.1. The security officer ensures that only one individual enters at a time. Personnel identification is established in accordance with paragraph 18.1.2.1. When the Fire Brigade is ready to enter the MAA or the vault, only the first person to enter the applicable area passes his/her Coded Credential Badge (Ref. 14) in front of the proximity reader as the CAS or the SAS de-energizes the electronic door strike. Access to the MAA or the vault is now unencumbered for the remainder of the Fire Brigade entering the respective area. Each new entry by the Fire Brigade to the respective area occurs in the same manner. In the event entry controls fail, all door locks fail open providing unencumbered access.

Reference 31 describes the procedures and controls for escorting visitors within the MAA and the vault. All personnel and materials, except as specified for emergency response, are subject to the contraband detecting measures

specified elsewhere in this plan. The response to suspected unauthorized personnel is in accordance with paragraph 18.1.2.1 of this plan.

#### 18.1.4 Bypass of Admittance Procedures and Controls

This section describes those measures employed to deter, delay, or deny attempts by an adversary using stealth or force to bypass admittance procedures and controls. Routine and nonroutine admittance measures, identified in Sections 18.1.2 and 18.1.3, respectively, provide some degree of protection and assurance that attempts to bypass entry controls by stealth or force are detected, assessed, and communicated. The following additional measures provide entry control points with the performance capability required by paragraph 73.45(b) of 10 CFR Part 73.

##### 1. Isolation Capabilities

The MAA control point is confined within the MAA and is isolated from the MAA by the entry/exit point designated MAA-1.1 (Figure 18-1). The structure is totally enclosed, permitting the passage of personnel and materials through only the MAA entry point and MAA entrance doors. Reference 66 describes the MAA control point in detail.

Personnel desiring access to the MAA are individually admitted to the MAA control point and are retained until the entire admittance operation is satisfactorily completed.

##### 2. Surveillance Capability

During open portal conditions, the MAA control point is continuously monitored from the CAS and the SAS by CCTV (Ref. 11). A Microwave Detection System (Ref. 56) provides continuous surveillance during closed portal operations. In the event a microwave detector annunciates, the MAA entry point is automatically monitored by CCTV from the CAS and the SAS for the purpose of verifying and assessing the alarm.

##### 3. Doors

Both doors to the MAA control point are interlocked to permit only one entry/exit door to be open at a time. Balanced Magnetic Switches (Ref. 6) alert the CAS and the SAS to each entry and exit event. The security officer inside the MAA control point also possesses the capability of locking each entry/exit point door while admitting or exiting functions are conducted.

Doors MAA-1.1, MEE-1.1, and VAU-1.1 are bullet resistant and afford a penetration-resistance equivalent, as a minimum, to the weakest component of the physical barrier (Refs. 21 and 28).

##### 4. Entry Control Personnel

Security officers performing entry control functions do not carry a weapon and are monitored by a duress sensor (Ref. 22) that annunciates in the CAS and the SAS. Only one security officer is present in the MAA control point at a time performing entry control functions. A second member of the entry control team monitors the MAA control point remotely by CCTV (Ref. 11) and can both detect and respond to a bypass attempt.

## 5. Penetration Resistance

The MAA entry point is constructed of materials presenting sufficient penetration resistance to allow the security officer time to ensure that MAA-1.1 is closed if an individual were passing through MAA-1.1 when the bypass attempt is initiated. Reference 66 describes the construction of the MAA entry/exit control point.

## 6. Response to a Bypass Attempt

The MAA control point security officer is instructed to delay and contain the adversary until response personnel arrive at the MAA control point. The reporting of and the response to an attempt to bypass admittance procedures and controls at an exit/entry control point is in accordance with Chapter 23 of this plan.

### 18.2 Entry Through Remainder of MAA/Vault Boundary

This section describes those measures employed to deter, delay, or deny attempts by an adversary to penetrate the physical barriers of the MAA or the vault. Physical barriers include walls, floors, ceilings, ventilation ducts (Ref. 3), and emergency exits (Ref. 28). Reference 38 describes the floor, ceiling, and walls. These protective functions provide assurance that such attempts using stealth or force are detected, assessed, and communicated and satisfy the performance capability requirements of paragraph 73.45(b).

#### 18.2.1 Detect Boundary Penetration Attempts

The physical barriers of both the MAA and the vault are monitored by components capable of sensing and alerting the CAS and the SAS of an attempted or actual penetration and facilitating assessment of such an occurrence. Table 18-8 identifies each of these components by function and specifies, when appropriate, whether the associated detection capability is primary (P) or diverse (D).

#### 18.2.2 Deter Boundary Penetration Attempts

The physical barriers of the MAA and the vault are fabricated from materials and erected in a manner that provides assurance that penetration attempts by an adversary are deterred. The incorporation of frequent Security Force patrols, adequate lighting, audible alarms, and unobstructed vision provides the perimeter of the physical barriers with an additional deterrence to penetration attempts. Table 18-9 identifies the various measures used to provide the MAA and the vault with positive deterrent capabilities.

#### 18.2.3 Response to Penetration Attempts

Security personnel respond to an actual or attempted penetration of a physical barrier in accordance with Chapter 23 of this plan. During the response phase of an actual or suspected penetration attempt, admittance to and all activities within the MAA and the vault are terminated. Normal operations are resumed only after the response force has established control of the penetration attempt or a surveillance component malfunction has been verified.

TABLE 18-1

WORK DESIGNATION CODES IDENTIFYING  
CATEGORIES OF ACTIVITIES INDIVIDUALS MAY BE  
AUTHORIZED TO PERFORM WITHIN AN MAA OR VAULT

<u>Work Designation Codes</u>	<u>Categories of Work</u>
A. <u>Employees</u>	
<u>LP</u>	<u>Licensee Personnel</u>
LP-1	Operations
LP-2	Maintenance
LP-3	Security
LP-4	Escort
LP-5	Management
LP-6	Administration
LP-7	Janitorial
LP-8	Health Physics
LP-9	Safety
LP-10	QA/QC
LP-11	Nuclear Technology
B. <u>Visitors</u>	
<u>SLP</u>	<u>State and Local Personnel</u>
SLP-1	LLEA
SLP-2	Fire
SLP-3	Governmental
<u>FO</u>	<u>Federal Officials</u>
FO-1	NRC Inspectors
FO-2	Other NRC Personnel
FO-3	IAEA
FO-4	Other Governmental
V-1	<u>All Others</u>

TABLE 18-2

SCHEDULE FOR IDENTIFYING ROUTINE  
WORKING AND NONWORKING TIME PERIODS

<u>Working Periods</u>	<u>Schedule Designation</u>
0001 - 0800	Swing Shift (SS)
0745 - 0815	Shift Change One (SC-1)
0801 - 1600	Day Shift (DS)
1545 - 1615	Shift Change Two (SC-2)
1601 - 2400	Night Shift (NS)
2345 - 0015	Shift Change Three (SC-3)
<u>Nonworking Periods</u>	<u>Schedule Designation</u>
0001 - 0800	Nonworking Period 1 (NWP-1)
0801 - 1600	Nonworking Period 2 (NWP-2)
1601 - 2400	Nonworking Period 3 (NWP-3)

TABLE 18-3

CRITERIA GOVERNING ACCESS AUTHORIZATION  
DURING ROUTINE WORKING AND NONWORKING PERIODS

	Working Periods	Working Periods Shift Changes	Nonworking Periods
1. Vaults will be locked.		+	+
2. General maintenance may be performed (excluding access authorization components).	+		
3. Access authorization components may be repaired, adjusted, calibrated, or replaced.			+
4. Entry/exit portals will be locked.		+	+
5. Materials may be allowed entry.	+		+*
6. SNM receipt and transfer operations may be performed.	+		
7. Maintenance may not be performed.		+	
8. Access control personnel may not be changed.		+	
9. Emergency exits will be locked.	+	+	+
10. No individual may be authorized entry unless escorted by Security Personnel.			+

\* Only for access authorization components.

TABLE 18-4  
METAL DETECTION

Object to be <u>Searched</u>	<u>LOCATION</u>	
	<u>Material Access Area Portal Designation Method</u>	<u>MAA-1.1 Reference</u>
1. Personnel	Walk Through	91 74
2. Unsealed Materials		
Clothing	Hand Held	89
Tools and Metallic Parts	Visual	
Instrumentation	Sealed*	81
Cleaning Materials	Hand Held	89
Boxes, Parcels, Packages	Hand Held	89
3. Sealed Packages**		

\* Tamper-indicating seals.

\*\* All sealed packages, except packages sealed with authorized tamper-indication seals, are opened prior to entry into the MAA.

TABLE 18-5  
EXPLOSIVE DETECTION

Object to be <u>Searched</u>	<u>LOCATION</u>	
	<u>Material Access Area Portal Designation Method</u>	<u>MAA-1.1 Reference</u>
1. Personnel	Hand Held	33
2. Unsealed Materials		
Clothing	Hand Held	32
Tools and Metallic Parts	Hand Held	32
Instrumentation	Hand Held	32
Cleaning Materials	Hand Held	32
Boxes, Parcels, Packages	Hand Held	32
3. Sealed Packages*	N/A	

\* All sealed packages are opened prior to entry into the MAA.

TABLE 18-6

NUCLEAR MATERIAL DETECTION

	<u>Object to be Searched</u>	<u>LOCATION</u>	
		<u>Material Portal Designation Method</u>	<u>Access Area MAA-1.1 Reference</u>
1.	Personnel	Hand Held	72
2.	Unsealed Materials		
	Clothing	Hand Held	72
	Tools and Metallic Parts	Hand Held	72
	Instrumentation	Hand Held	72
	Cleaning Materials	Hand Held	72
	Boxes, Parcels, Packages	Hand Held	72
3.	Sealed Packages*	N/A	

---

\* All sealed packages are opened prior to entry into the MAA.

TABLE 18-7

WORK DESIGNATION CODES IDENTIFYING NONROUTINE  
 RESPONSE ACTIVITIES INDIVIDUALS MAY BE  
AUTHORIZED TO PERFORM WITHIN AN MAA OR VAULT

<u>Work Designation Codes</u>	<u>Response Activities</u>
	A. Emergencies
A1	Fire
A2	Personnel Injury
A3	Explosion
A4	Radiological
A5	Chemical
A6	Bomb Threat
A7	Material Loss etc.
	B. Production
B1	Equipment Failure
B2	Equipment Malfunction
B3	Leaks
B4	Stoppages and Blocking etc.
	C. Environmental
C1	Lighting
C2	Heating
C3	Air Conditioning
C4	Plumbing etc.

TABLE 18-8

COMPONENTS USED FOR SENSING, TRANSMITTING,  
AND ASSESSING PHYSICAL BARRIER PENETRATION ATTEMPTS

SENSING

<u>Area</u>	<u>Type</u>	<u>Reference</u>
MAA	*(P) Microwave Systems	56
	(D) Video Motion Systems	11
Vault	(P) Microwave Systems	56
	(D) Video Motion Systems	11

TRANSMITTING

<u>Systems</u>	<u>Type</u>	<u>Reference</u>
Microwave	(P) Individual Hardwire	47
	(D) Multiplexed Hardwire	47
Video Motion	(P) Individual Hardwire Video	47

ASSESSING

<u>Area</u>	<u>Type</u>	<u>Reference</u>
MAA	(P) CCTV Surveillance	10
	(D) Patrols	43
Vault	(P) CCTV Surveillance	10
	(D) Patrols	43

\* P means primary; D means diverse.

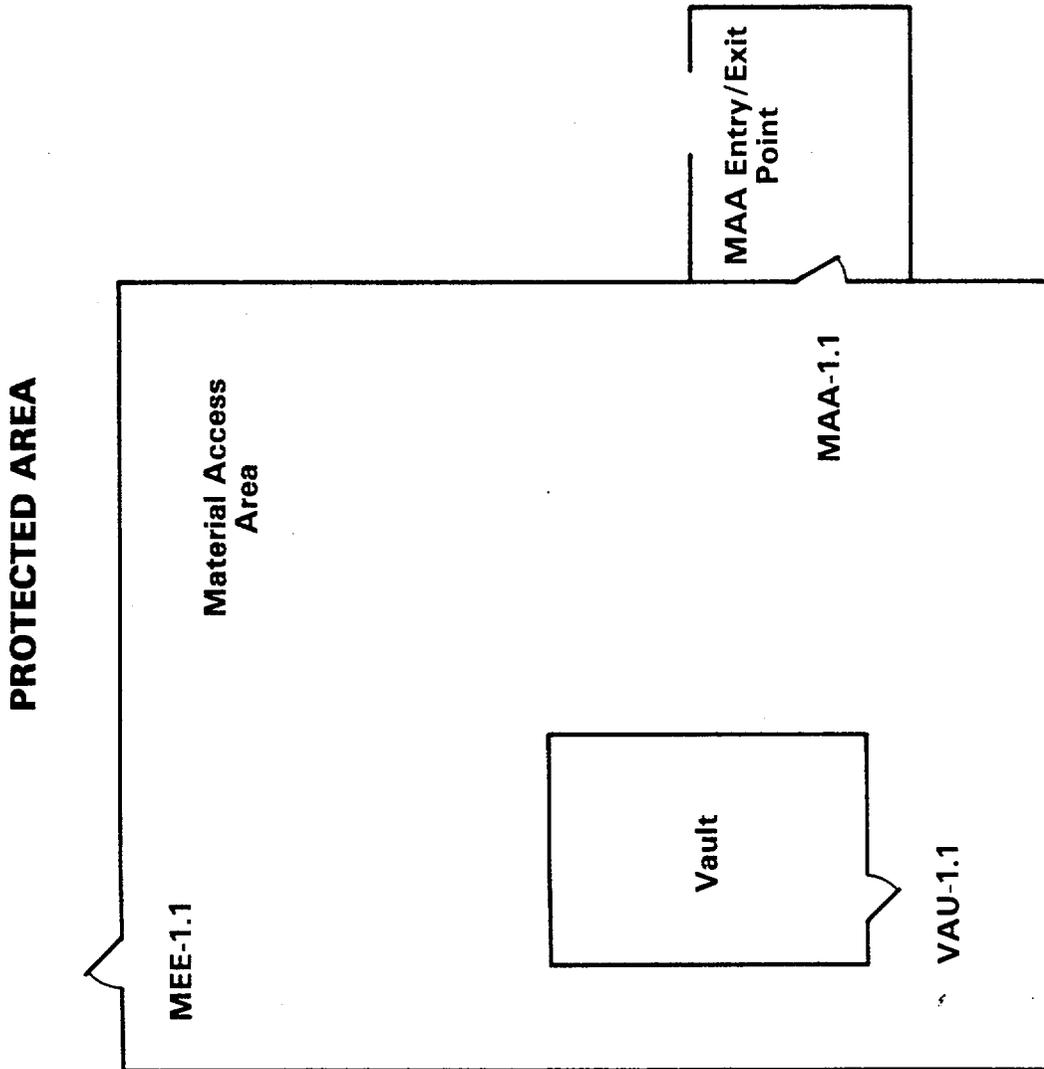
TABLE 18-9

MEASURES USED TO DETER ADVERSARY PENETRATION ATTEMPTS

<u>Area</u>	<u>Type of Measure</u>	<u>Reference</u>
MAA	Barriers (Walls)	38
	Patrols	43
	Lighting	17
	Alarms (Microwave)	56
	(Video Motion)	11
Vault	Barriers (Walls)	38
	Lighting	17
	Alarms (Microwave)	56
	(Video Motion)	11

FIGURE 18-1

MAA AND VAULT BLOCK DIAGRAM



## APPENDIX 1 TO ATTACHMENT A

Reference 1

### Admittance Authorization Criteria and Schedules

#### 1. Function

Admittance authorization criteria and schedules are developed for the purpose of determining what activities are authorized, who is authorized to perform them, and when these activities are authorized to be performed. They are used in determining authorized access to the protected area and material access areas at all times that access may be required.

#### 2. Responsible Personnel

The criteria and schedules are formulated and authorized by the following individuals:

- |                                  |   |
|----------------------------------|---|
| (1) Personnel Manager            | (7) Safety and Environmental Control Department Manager |
| (2) Training Manager             | (8) Plant Manager                                       |
| (3) Health Physics Manager       | (9) Production Superintendent                           |
| (4) Security Manager             | (10) Security Shift Supervisor                          |
| (5) Site Emergency Director      |   |
| (6) Physical Security Supervisor |   |

(See #4 for specific functions performed.)

#### 3. Verification and Audit

Admittance authorization criteria and schedules are incorporated into a computerized admittance criteria screening process. Access authorization is verified by computer program that matches two different authorization data files (Ref. 2). Verification and audit of the input of criteria and schedule changes are accomplished as part of the normal generation of work and shift schedules, which are then crosschecked against production schedules and area authorization criteria. If any one of the independently generated schedules is not properly executed, the computer programming will not allow access and an audit of schedule generation results. Additionally, daily checks of all shift schedule changes are conducted by the Security Manager and monthly checks of all schedule and criteria changes and supporting documentation are made by the Quality Assurance/Control department.

#### 4. Operation and Performance

a. Personnel authorization criteria used include individual status (employee/visitor), radiation safety training, security clearance level, work designation codes, emergency work designation codes, and work periods authorized.

b. Material authorization criteria are contained in the Security Work Order. An inventory of necessary materials that specifies what materials are needed and allowed in PAs, VAs, and MAAs, based on each specific area's operational and support requirements, is maintained.

c. Area authorization criteria include individual status (employee/visitor), radiation safety training required, security clearance required, designation of authorized activities, and periods activities are authorized to be performed (by area).

d. The criteria for personnel are entered into the computer as one data file. The criteria for areas are entered as a second data file. Schedule data are developed from production schedules, shift schedules, and work designation codes and determine the minimum numbers and kinds of personnel who will require access to specific areas, based on operational and support requirements.

e. The criteria described above are supplied to the computer by the individuals identified in #2 above. The data are supplied for personnel and area data files and entered by different individuals as follows:

#### Personnel File

Personnel Manager - develops work designation codes and individual's status;

Training Manager - develops basic safety training criteria;

Health Physics Manager - develops advanced safety training criteria;

Security Manager - identifies security clearance data;

Site Emergency Director - develops emergency work designation codes;

Physical Security Supervisor - develops work period criteria.

#### Area File

Physical Security Supervisor - individual status (employee/visitor);

Safety and Environmental Control Department Manager - develops area radiation safety training requirements;

Security Manager - develops security clearance levels required per area;

Plant Manager - develops area work designation codes;

Production Superintendent - develops work period criteria per area;

Security Shift Supervisor - develops area emergency work designation codes.

f. Emergency work designation codes are developed using the criteria established in the Contingency Plan and Procedures (Ref. 16).

g. System design and performance are such that in establishing a new access authorization if any one of the criteria is not properly met, admittance is denied. When access authorization is to be terminated, if only one of all the criteria is changed to cancel authorization, further admittance is denied. Therefore, a single discrepancy, either inadvertent or deliberate, will deny access for new authorizations and deny admittance for cancelled authorizations.

h. Documentation supporting criteria and schedules is kept independently by those individuals responsible for development. Such documentation includes training records, personnel records, health physics records, approved shift and production schedules, and material transfer records.

5. In addition to the collusion protection provided by having criteria and schedules developed and entered by separate individuals and independently audited monthly, computer terminals use password protection to minimize the possibility of a knowledgeable individual defeating the system. The criteria and schedule system is designed so that defeat would require collusion on the part of three individuals.

Coded Credential System

1. Function and Description

The coded credential system is used to verify admittance authorization to the PA and the MAA. The system is a Schlage Model 414, which uses proximity readers and a passive electronic badge system. In addition to the primary function, the system is also used to activate personnel identification image files and to account for personnel presence in various onsite areas.

2. Capabilities and Operation

The system is capable of processing 1500 different badge codes. It is used as part of access control at all entrances to the PA, MAA, and MAA vault. It functions and operates as follows:

a. An issued badge is placed within proximity of a reader. The individual wishing access also provides his company ID number on the associated processor. The entered credential code and proper ID number are used to trigger the computerized admittance authorization system (Ref. 1) which verifies that the individual is authorized access to the area being entered. Proper verification allows entrance to the appropriate entry/exit control point where search and further identification is then conducted.

b. The proper credential code and employee ID number combination also triggers a computerized video-stored image file for use by entry/exit control-point security personnel as the primary means of identification. The credential code ID number combination is used to select the correct video facial image from a video storage file for placement on a video monitor in the appropriate exit/entry control point. Security personnel then compare this image to the face of the individual seeking entry.

c. The coded credential system is also capable of actuating a personnel inventory printout, which will identify which individuals are located in which onsite areas.

d. Credentials are maintained on site. The system could be vulnerable to substitution of similar credentials only if the substituted code was identical to one already enrolled in the system and only if that code was not being used at the same time. An antipassback feature disallows the use of one code for more than one entry into an area.

3. Accountability

The credentials are kept within the PA entry/exit control point. Upon entry, an employee is issued a credential and enters the employee ID number into the computer. The computer matches the credential code to the ID number and uses this combination for all other entries during the employee's time on site. The credential is returned when the individual leaves the site. Loss of a credential results in that code being programmed so that future use is rejected by the system. A daily check of issuance/return records is made (the

computer logs discrepancies) by the Physical Security Supervisor. A monthly physical count of all credentials is also conducted as an audit measure.

4. In the event of system failure, documentation normally used to program the computer is provided to entry/exit control-point personnel. Access authorization is conducted using these records. If the video image file fails, picture badges are used as a substitute for personnel identification.

5. Preventive maintenance is conducted in accordance with manufacturer's specifications. Operational checks are conducted continually as part of normal operation. Security personnel perform operational checks; maintenance is conducted by maintenance technicians.

6. The system does not use equipment or line tamper protection.

Duress Alarms

1. Function and Description

Duress alarms communicate a threatening situation when activated by a security officer.

A duress alarm consists of a miniaturized transmitter, a panic button, and a battery pack worn by the security officer.

All security officers manning MAA entry/exit control points are monitored by duress alarms. These alarms are concealed under the clothing of the security officer.

Security officers are issued duress alarms prior to assuming responsibility for entry control functions. After the alarm is in place, it is tested to ensure proper operation prior to the security officer's assuming entry control duties.

The environmental conditions of each MAA control point are controlled such that they do not adversely affect the performance of the duress alarms. Additionally, because of the resistance of the physical barriers of the facility to RF transmissions, RF receivers are installed inside each MAA. The RF receivers are hardwired to the CAS and the SAS to ensure the transmission of alarm signals out of the facility.

2. Operation

Activation of the panic button initiates an RF signal that is picked up by a receiver in the MAA and transmitted by hardwire to the CAS and the SAS.

Duress alarms annunciate with both audible and visual indications at the CAS and the SAS. A common audible alarm alerts the monitor to the occurrence of a duress alarm. Individual visual displays alert the monitor to the specific location of the duress alarm.

An alarm condition is assessed by security officers patrolling the area (Ref. 43) and remotely by CCTV (Ref. 10) from the CAS and the SAS.

Security officers are continuously required to interact with the computer processor, via the communications terminal, prior to the individual's gaining access to the MAA. When the security officer perceives a threat, he/she alerts the CAS and the SAS by entering an alert code on the communication terminal. This serves as a redundant duress alarm.

3. Maintenance and Testing

All maintenance is performed by Technical Security Officers.

Corrective maintenance is performed on an as-needed basis.

Preventive maintenance is performed at least every 3 months or more frequently when indicated by the manufacturer's maintenance instructions. Duress alarms inside the MAA control point are tested at the beginning of each shift. The test is conducted by having the security officer activate the device prior to assuming duties.

4. Vulnerability

The manner in which the security officer perceives the threat and the training he has received for responding to a stress situation affect the reliability of the duress alarm.

Motion Detectors - Interior Microwave Systems

1. Function and Description

The microwave detection system provides the capability for detecting adversary activities within the MAA during closed portal conditions.

The Advanced Device Laboratories (ADL), Model 3300, Microwave Motion Detection System is employed. The motion detection system uses a doppler, microwave unit. Movement is detected by a shift in the transmitted frequency. The extent of frequency shift is a function of the size of the target and the speed at which the target is moving through the microwave beam. The ADL Microwave Detection System is capable of detecting a 3-square-foot object moving within the MAA at a rate varying from 3 inches per second to 10 miles per hour. When motion is detected, the microwave unit annunciates audibly and visually, both remotely and locally. Remote annunciation is in the CAS and the SAS. The system has a greater than 99 percent probability of detection and less than 0.5 percent probability of initiating a false alarm.

2. Installation and Site Conditions

Microwave motion detection units are positioned within the area of coverage such that blind spots on the floor, ceiling, and walls are eliminated. See Reference 38 for a physical description of the physical barriers.

For areas having a height of 20 feet or less, microwave units are normally positioned at a height varying from 12 to 14 feet. A minimum of 9 feet is always maintained unless lower levels are specifically required. For areas having a height of 21 feet or greater, microwave units are positioned to provide multiple detection levels.

a. Man-made environmental conditions, including temperatures, are all controlled so that they do not adversely affect the proper operation of the microwave detection units. The ADL microwave detection unit functions between -20 and +120 degrees Fahrenheit with almost zero false alarm rate.

b. Electromagnetic interference (EMI) protection is provided by restricting RF radiating equipment inside the MAA during closed portal conditions. Fluorescent lighting fixtures are not positioned within 5 feet of a microwave motion detection unit.

The MAA control point, MAA, and vault are each located inside the facility. Therefore, natural phenomena are not expected to adversely affect the proper operation of the ADL Microwave Detection System. Lightning protection is provided by the facility design considerations and power line filtering.

All microwave detection units are mounted on stable surfaces such as the wall or ceiling (Ref. 38).

### 3. Power Supplies

Each microwave detection unit contains a 12-volt rechargeable battery that is capable of operating the unit for 4 hours upon a loss of normal power. Additionally, microwave detection units are connected to the Emergency Generating System which is capable of providing electrical power within 15 seconds of a loss of normal power and for a period of 30 days.

Microwave detection units are only operated during closed portal conditions. Units are positioned and adjusted so that the area of coverage is overlapped. Microwave beams are adjusted so that one beam does not interact with another microwave detection unit.

### 4. Redundant Systems

The CCTV Video Motion Detection System (Ref. 11) during both opened and closed portal conditions provides redundant and diverse motion detection in applicable areas. Additionally, security force officers continuously patrol the peripheral areas of the MAA (Ref. 43).

### 5. Assessment

Each microwave unit is connected to a CCTV camera (Ref. 11). When motion is detected, the CCTV camera is automatically activated to produce a visual display of that area in which motion was detected. Remote alarm assessment of an alarm condition or potential adversary action is performed by the CAS and the SAS.

Local assessment is performed by security officers patrolling the VA and by response personnel (Ref. 43).

### 6. Maintenance and Testing

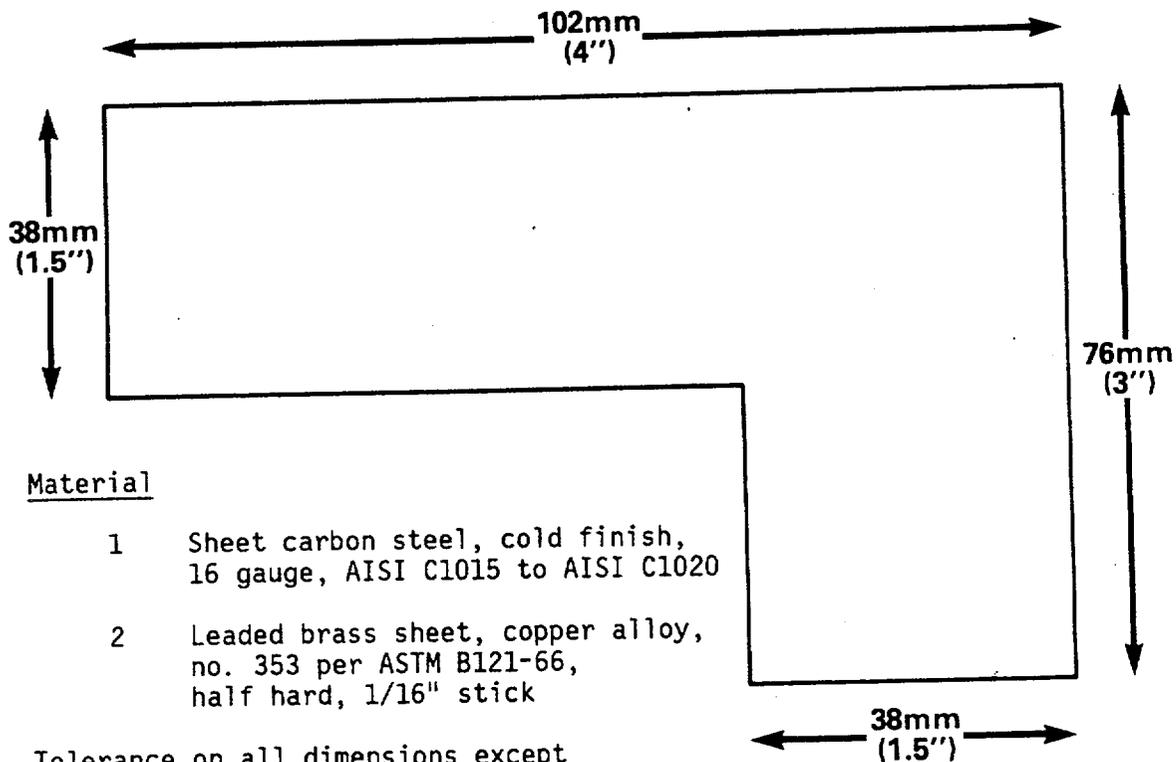
All maintenance is performed by Technical Security Officers.

Weapons Detector, Hand-Held, Package and Personnel Search1. Function

The listed hand-held weapon detectors will be used as a redundant component for the detection of metal contraband entering the MAA.

2. Calibration Testing

The detector will detect test objects 1 and 2 as pictured below which simulate .25 semiautomatic pistols. In addition, the detector will detect a third test object consisting of a stainless steel double-edged razor blade with nominal thickness of .1 mm (.004"). Separation distances from the detector for calibration purposes are 3" for test objects 1 and 2 and 1" for test object 3. All the test objects will be detected with a 99 percent probability with an associated false alarm rate of .1 percent. Both primary and redundant detectors will be calibration tested within 30 minutes prior to each shift change.

Material

- 1 Sheet carbon steel, cold finish, 16 gauge, AISI C1015 to AISI C1020
- 2 Leaded brass sheet, copper alloy, no. 353 per ASTM B121-66, half hard, 1/16" stick

Tolerance on all dimensions except material thickness  $\pm 1$  mm ( $\pm 0.04$ " )

3. Operating Procedures

(To be used in event of failure of walk-through detector)

a. Two detectors will be available. One will be used as a redundant, backup detector in the event of primary detector failure.

b. Each person to be searched will be asked to remove articles such as bulky overcoats or raincoats that may be used to conceal contraband.

c. Each person subject to search will also be asked to surrender all hand-carried items. These hand-carried items will be searched in accordance with Reference 89 or by the hand-held metal detector.

d. Prior to each search sequence, the detector operation will be considered satisfactory if the detector alarms when passed over any one of the three calibration standards. This procedure will be considered the operational test.

e. If the primary detector does not pass the operational test, the search will be conducted using the "redundant" detector until the primary detector is either replaced or recalibrated. If both the primary and redundant detectors fail or malfunction, a "pat-down" search will be conducted in accordance with Reference 59.

f. The hand-held detector will be run over all parts of the body, including hands, arms, underarms, chest, back, lower body, legs, and feet.

g. Upon successful completion of the search without an unresolved alarm, the individual will be subjected to the next step in the authorization process.

h. If the detector alarms and the alarm is unresolved, the person being subjected to the search will be searched using the redundant detector. If no alarm occurs, the individual will be allowed to proceed to the next admittance authorization function. If an alarm occurs, the individual will be subjected to a pat-down search.

i. If the pat-down search is positive, the individual will immediately be placed in isolation and a response initiated in accordance with Reference 16.

#### 4. Redundant Measures

Redundant equipment used in the event of an equipment failure is as shown in response to #1 above. Pat-down searches in accordance with Reference 59 may also be used in the event of primary and redundant alarm failure.

#### 5. Test and Maintenance

No specific preventive maintenance program is planned other than to replace the batteries as required. Operational tests and inspections will be accomplished to verify operation of the hand-held weapon detector by passing the detector over one of three aforementioned test objects before each search. If any of these test objects causes the detector to alarm, the performance of the detector is acceptable. Calibration tests will be conducted as stated in #2 above.

INFORMATION REQUEST SHEETS REFERENCED IN SAMPLE PORTION OF PLAN

1. Admittance Authorization Criteria and Schedules
2. Admittance Authorization and Verification Procedures
3. Air and Utility Inlet Barriers
6. Balanced Magnetic Switches
10. CCTV Monitoring/Surveillance
11. CCTV Systems
14. Coded Credential System
16. Contingency Plans and Procedures
17. Controlled Security Lighting
21. Doors and Associated Hardware
22. Duress Alarms
28. Emergency Exits
31. Escorts
32. Explosive Detector, Hand-Held, Package Search
33. Explosive Detector, Hand-Held, Personnel Search
38. Floors, Roofs, and Walls
43. Guard Patrols and Intervention
47. Interface Between Alarm Station and Sensors--Individual Hardwire Alarms, Multiplexed Hardwire Alarms, and Hardwire Command Signals
56. Motion Detectors--Interior Microwave Systems
69. Pat-Down Search
64. Positive Personnel Identity Verification
66. Sally Ports, Pedestrian
72. SNM Detectors, Hand-Held, Personnel Search
81. Tamper-Indicating Seals and Tamper-Seal Inspection
84. Vaults
86. Visual Inspection, Package Search
89. Weapons Detector, Hand-Held, Package and Personnel Search
91. Weapons Detector, Walk-Through

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

