DOE M 473.1-1

Approved: 12-23-02

PHYSICAL PROTECTION PROGRAM MANUAL

U.S. DEPARTMENT OF ENERGY

Office of Security

DISTRIBUTION:
All Departmental Elements

INITIATED BY:
Office of Security

PHYSICAL PROTECTION PROGRAM MANUAL

FOREWORD

1. PURPOSE. This Manual supplements DOE O 473.1, *Physical Protection Program,* dated 12-23-02, by establishing requirements for the physical protection of safeguards and security (S&S) interests.

2. CANCELLATION. DOE M 5632.1C-1, *Manual for the Protection and Control of Safeguards and Security Interests,* dated 7-15-94. Cancellation of the specified Manual does not modify or otherwise affect any contractual obligation to comply with the DOE requirements. If a cancelled Manual or chapter is incorporated by reference in a contract, it remains in effect until the contract is modified to delete the reference to the requirements in the cancelled Manual or chapter.

3. APPLICABILITY.

   a. DOE Elements. This Manual applies to all Department of Energy (DOE) elements, including the National Nuclear Security Administration (NNSA), as listed on Attachment 1.

   b. Site/Facility Management Contractors.

      (1) As indicated in the Contractor Requirements Document (CRD), Attachment 2, all parts of this Manual are relevant and applicable to contractors responsible for the management and operation of DOE-owned facilities (hereafter referred to as site/facility management contractors) whose contracts include the CRD.

      (2) The CRD, which incorporates the requirements of this Manual by reference, must be included in site/facility management contracts that contain DOE Acquisition Regulation (DEAR) clause 952.204-2, Security Requirements.

      (3) This Manual does not automatically apply to other than site/facility management contracts. Application of any of the requirements of this Manual to other than site/facility management contracts will be communicated separately from this Manual as follows.

         (a) Lead Program Secretarial Officers. Must notify contracting officers to incorporate this Manual into affected site/facility management contracts.
         (b) Contracting Officers.

1 Once notified, are responsible for incorporating this Manual into the affected contracts via the laws, Regulations, and DOE directives clause of the contracts.

2 Assist originators of procurement requests who want to incorporate the clause at 48 CFR 952.204-2, Security Requirements, and the requirements of this Manual in new non-site-/non-facility-management contracts, as appropriate.

c. Exclusions. None.

4. REFERENCES. Relevant references are in Attachment 3.

5. CONTACT. Questions concerning this Manual should be directed to the program manager, Protection Program Operations, at 301-903-6209.

6. IMPLEMENTATION. Requirements that cannot be implemented within 6 months of the effective date of this Manual or within existing resources must be documented by the head of the field element and submitted to the relevant program office; the Under Secretary for Energy, Science and Environment or the Administrator, NNSA; and the Office of Security.

BY ORDER OF THE SECRETARY OF ENERGY:

KYLE E. McSLARROW
Deputy Secretary

CONTENTS

CONTENTS (continued)

CONTENTS (continued)

CONTENTS (continued)

ATTACHMENTS

TABLES

CHAPTER I.

PROTECTION PLANNING

1. PLANNING. The implementation of graded physical protection programs required by this Manual must be documented. Physical protection programs must be systematically planned, executed, and evaluated. (See DOE O 470.1, *Safeguards and Security Program,* dated 9-28-95.)

   a. In locations where a Site Safeguards and Security Plan (SSSP) is not required due to the limited scope of safeguards and security (S&S) interests, a security plan must be developed to describe the protection program.

   b. The "Design Basis Threat for the Department of Energy Programs and Facilities (U)," issued by the Office of Security, must be used in conjunction with local and regional threat guidance and vulnerability assessments for physical protection program planning.

2. PROTECTION STRATEGIES. Protection strategies must be selected, developed, and implemented to protect S&S interests. (See DOE O 470.1.)

3. GRADED PROTECTION. Protection must be applied in a graded manner, commensurate with provisions of S&S program policy. (See DOE O 470.1.)

4. PERFORMANCE ASSURANCE. Physical protection systems, including components, must be tested to ensure overall system effectiveness. (See DOE O 470.1.)

5. SAFETY AND HEALTH. S&S programs must meet mission objectives and the DOE safety and health objectives to protect workers. The health and safety of workers is paramount; all reasonable means of protecting workers must be followed to ensure national security assets remain protected.

This page intentionally left blank.

CHAPTER II.

PROTECTION OF NUCLEAR WEAPONS AND SPECIAL NUCLEAR MATERIALS

1. GENERAL REQUIREMENTS. This chapter defines requirements for protecting nuclear weapons and Category I through IV quantities of special nuclear material (SNM). The priority of protection measures must be designed to prevent malevolent acts such as theft and radiological sabotage, and to respond to adverse acts such as emergencies caused by acts of nature.

   a. A facility may not possess, receive, process, transport, or store nuclear weapons or SNM until that facility has been cleared. (See DOE O 470.1.)

   b. An integrated, graded system of positive measures must be developed and implemented to protect Category I and II quantities of SNM and nuclear weapons. Protection measures must address physical protection strategies of denial and containment as well as recapture, recovery, and/or pursuit.

   c. Physical protection for each category of SNM must consider the following factors: quantities, chemical forms, and isotopic composition purities; ease of separability, accessibility, concealment, and portability; protection strategies; radioactivity; and self-protecting features.

   d. The protection of nuclear material production, reactors, and fuel must be consistent with the category of SNM involved and/or the consequences of radiological sabotage.

   e. SNM or explosives that are classified because of their configuration or content, or because they are part of a classified item, must receive the physical protection required by the highest level of classification or category of SNM involved.

   f. Specific physical protection measures and protective force (PF) response capabilities needed to comply with protection requirements must be described in an SSSP or a security plan.

   g. Protection afforded SNM must be graded according to the nuclear material safeguards category and attractiveness and must reflect the specific nature of the nuclear weapons or SNM at each site. For facilities where roll-up (i.e., the accumulation of smaller quantities of SNM) is credible, SNM must be protected at the higher category level, unless the facility has conducted a vulnerability assessment that determined that failure or defeat of protection measures will not increase the risk. (See DOE M 474.1-1A, *Manual for Control and Accountability of Nuclear Materials,* dated 11-22-00.)

2. ACCESS. Access controls must be in place to ensure that only cleared and authorized personnel are permitted unescorted access to SNM and nuclear weapons. Access authorizations must be granted in accordance with DOE O 472.1B, *Personnel Security Activities,* dated 3-24-97. The types of access authorization required for unescorted access is shown in Table 1.

Table 1. Access Authorization Requirements for Unescorted Access to SNM

Special Nuclear Materials Category	Type of Access Authorization Required for Unescorted Access	Remarks
I and II with roll-up to I	Q	Hands-on access or transportation of Category I quantities of SNM will require additional measures, such as participation in a human reliability program and/or enhanced material surveillance procedures, to further reduce the probability of insider acts. Document in the SSSP.
II and III	L	Unless special circumstances determined by the site vulnerability assessment requires a Q access authorization to minimize risk. Document in SSSP or security plan.
IV	None	Unless special circumstances determined by the site vulnerability assessment, requires an access authorization to mitigate risk. Document in SSSP or security plan.

3. INTRUSION DETECTION SYSTEM. Category I and II quantities of SNM and nuclear weapons must be protected by an integrated physical protection system using PFs, barriers, and intrusion detection systems (IDSs).

4. DELAY MECHANISMS (BARRIERS). Delay mechanisms must be employed to delay access, removal or unauthorized use of Category I and II quantities of SNM and nuclear weapons. Delay mechanisms may include both passive physical barriers (e.g., walls, ceilings, floors, windows, doors, and security bars) and activated barriers (e.g., sticky foam, pop-up barriers, and cold smoke).

5. PROTECTIVE FORCE. A PF program must be established. A response capability must be maintained to deny, neutralize, contain, and/or perform recapture/recovery and pursuit missions within the required response times. (See DOE O 473.2, *Protective Force Program,* dated 6-30-00.)

6. STORAGE CONTROLS. Each facility must have controls for SNM and nuclear weapons held in storage consistent with the graded safeguards approach required by paragraphs 7 through 10. Controls for storage must—

   a. be documented,

   b. ensure that only authorized personnel have access to the storage repositories,

   c. detect unauthorized access,

   d. authenticate SNM movements into or out of a storage location,

   e. include procedures for investigating and reporting abnormal conditions,

   f. provide a record system to document ingress into and egress from storage, and

   g. define procedures for conducting inventories and daily administrative checks.

7. CATEGORY I SPECIAL NUCLEAR MATERIAL. The following requirements apply to the use or processing, storage, and transportation of Category I quantities of SNM.

   a. Use or Processing. Category I quantities of SNM are to be located within material access areas (MAAs), inside a protected area (PA). Any location within an MAA that contains unattended Category I quantities of SNM in use or process must be equipped with IDS or other effective means of detection approved by the cognizant DOE authority.

   b. Storage. Category I quantities of SNM that are not in use or process must be stored within an MAA as follows.

      (1) Category I, Attractiveness Level A SNM must be stored in a vault. Storage facilities constructed after 7-15-94 for Category I Attractiveness Level A SNM must be underground or below-grade.

(2) Category I, Attractiveness Level B SNM must be stored in a vault or provided enhanced protection that exceeds vault-type room storage (e.g., collocated with a PF response station and/or activated barriers).

(3) Category I, Attractiveness Level C SNM must, as a minimum, be stored in a vault-type room.

c. Transportation. The following requirements apply to the protection of Category I quantities of SNM being transported.

(1) Domestic offsite SNM shipments must be made by the Office of Transportation Safeguards.

(2) Packages or containers containing the SNM must be sealed with tamper-indicating devices.

(3) To protect against the threats described in the "Design Basis Threat for Department of Energy Programs and Facilities (U)," protection measures for movements of the SNM between PAs at the same site, or between PAs and staging areas at the same site, must be under constant surveillance by armed PF escort personnel.

8. CATEGORY II SPECIAL NUCLEAR MATERIAL. The following requirements apply to the use or processing, storing, and transport of Category II quantities of SNM.

a. Use or Processing. Category II quantities of SNM must be located within a PA and under material surveillance.

b. Storage. When not in use or process, Category II quantities of SNM must be stored in a vault or vault-type room located within a PA.

c. Transportation. Shipments of Category II quantities of SNM must conform to the requirements prescribed in paragraph 7c above.

9. CATEGORY III SPECIAL NUCLEAR MATERIAL. The following requirements apply to use or processing, storage, and transportation of Category III quantities of SNM.

a. Use or Processing. Category III quantities of SNM must be used or processed within a limited area.

b. Storage. When not in use or process or when unattended, Category III quantities of SNM must be stored within a locked security container or locked room that is located within the minimum of a limited area. The container or locked room containing the SNM must be under the protection of an IDS or physical check by a PF patrol at least every 8 hours.

c. Transportation. Category III quantities of SNM may be transported by the following methods unless otherwise prohibited by statute.

(1) Domestic offsite shipments of classified configurations of Category III quantities of SNM must be made by the Office of Transportation Safeguards.

(2) Authorized methods of shipping unclassified configurations when not made by the Office of Transportation Safeguards.

(a) Truck or train shipments must meet the following requirements.

1 Government-owned or exclusive-use truck, commercial carrier, or rail may be used to ship unclassified configurations of Category III quantities of SNM.

2 The transport vehicle must be inspected in detail before loading and shipment. Cargo compartments must be locked and sealed after inspection and remain sealed while en route.

3 Shipment escorts must periodically communicate with a control station operator. The control station operator must be capable of requesting appropriate local law enforcement agency response, if needed.

4 Shipments must be made without intermediate stops except for emergencies, driver relief, meals, refueling, or transfer of security interests.

(b) Unclassified configurations of Category III quantities of SNM may be shipped by air. Shipments must be under the direct observation of the authorized escorts during all land movements and loading and unloading operations.

(3) Movements of Category III quantities of SNM between security areas at the same site must comply with the locally-developed security plan.

10. CATEGORY IV SPECIAL NUCLEAR MATERIAL. The following requirements apply to the use or processing, storage, and transportation of Category IV quantities of SNM.

a. Use or Processing. Category IV quantities of SNM must be used or processed in accordance with local security procedures approved by the cognizant DOE authority.

b. Storage. When not in use or process or when unattended, the SNM must be stored in a locked area and procedures documented in an approved security plan.

c. Transportation. Category IV quantities of SNM may be transported by the following methods unless otherwise prohibited by statute.

(1) Domestic offsite shipments of classified configurations of Category IV quantities of SNM may be made by the Office of Transportation Safeguards, or by other means when approved by the respective heads of field elements.

(2) Shipments of unclassified Category IV quantities of SNM may be made by truck, rail, air, or water craft in commercial for-hire or leased vehicles.

(a) Shipments (except laboratory analysis samples or reference materials) must be by a mode of transportation that can trace and identify, within 24 hours of request, the precise location where a shipment went astray in the event it fails to arrive at the destination at the prescribed time.

(b) Shippers are required to give the consignee an estimated time of arrival before dispatch and to follow up with a written confirmation not later than 48 hours after dispatch.

(c) Consignees must promptly notify the shipper by telephone and written confirmation upon determination that a shipment has not arrived by the scheduled time.

11. VITAL EQUIPMENT. Site SSSPs must define applicable threats and measures to protect Vital Equipment from hostile actions.

CHAPTER III.

PROTECTION OF CLASSIFIED MATTER

The following are general requirements for the protection of classified matter. Detailed requirements for the protection of classified matter are in DOE 471.2 series policy documents.

1. Classified matter is any combination of documents and material containing classified information. This includes classified parts and explosives whose shapes are considered classified. Classified SNM must be protected in accordance with Chapter II. The secure storage requirements are described in Chapter XI.

2. Classified matter must be processed, handled, or stored in security areas providing protection measures equal to or greater than those present in a limited area in accordance with Chapter V.

3. Classification levels must be used in determining the degree of protection and control required for classified matter. Custodians and authorized users of classified matter are responsible for the protection and control of such matter.

4. Access to classified matter must be limited to persons who possess appropriate access authorization and who require such access (need to know) in the performance of official duties. Controls must be established to detect and deter unauthorized access to classified matter.

5. Buildings and rooms containing classified matter must be afforded the security measures necessary to deter unauthorized persons from gaining access to classified matter, specifically to include security measures to deter persons outside the facility protective zone from viewing or hearing classified information. Conference rooms and areas specifically designated for classified discussions must follow Technical Surveillance Countermeasures Program requirements. (See the DOE *Technical Surveillance Countermeasures Procedural Manual (U),* dated 10-94.)

6. When size, weight, construction, radiation, or characteristic make standard storage impractical, the field activity is authorized to approve protection measures that provide equivalent protection. If equivalent protection cannot be provided, the deviation process outlined in DOE 470.1 must be followed.

This page intentionally left blank.

CHAPTER IV.

RADIOLOGICAL, CHEMICAL, AND BIOLOGICAL SABOTAGE PROTECTION

1. GENERAL REQUIREMENTS. This chapter provides the requirements for a radiological, chemical and biological sabotage protection program. The physical protection of SNM must be in accordance with Chapter II and this chapter.

   a. The site/facility must ensure that S&S functions for radiological/chemical/biological sabotage protection are coordinated and integrated into its emergency management plan and radiation protection program.

   b. SNM identified as radiological/chemical/biological sabotage targets must provide protection as determined by vulnerability analysis.

2. ANALYSIS. Facilities with a radiological/chemical/biological sabotage threat must document the sabotage analysis process and the program for protection in a SSSP or a security plan.

   a. Analysis. Radiological/chemical/biological sabotage analysis must consider a wide variety of factors, such as materials, locations, site-specific features, and existing security, safety, and mitigation features.

   b. Emergency and Safety. Safety analysis reports, Emergency Planning Hazards Assessments (see DOE O 151.1A, *Comprehensive Emergency Management System,* dated 11-01-00), vulnerability analysis reports, accident scenarios, emergency event classifications, protective actions, consequence calculations, and other pertinent information should be considered in the radiological/chemical/biological sabotage analysis. The site emergency management plans and procedures for mitigation of events must also be considered when developing security plans and planning documents for radiological/chemical/biological sabotage.

3. RADIOLOGICAL/CHEMICAL/BIOLOGICAL SABOTAGE. Physical protection strategies must be developed, documented, and implemented to protect radiological/chemical/biological sabotage targets.

   a. Radiological. Protection must be provided in a graded manner, consistent with the level of hazards present, to protect S&S interests and to mitigate consequences of a radiological sabotage event.

   b. Chemical/Biological. Chemical/biological sabotage targets may be protected at a level that is equivalent to the protection provided by industry or private commerce to ensure public health and safety.

c. Mitigation. The following prevention and mitigation options must be implemented in a graded manner based on the results of the radiological/chemical/biological sabotage analysis:

(1) S&S features to detect or delay adversary actions (i.e., access and materials controls, surveillance, additional barriers/alarms, and entry/exit inspections);

(2) additional controls or equipment that would prevent a sabotage release scenario (e.g., providing automatic shutdown if components fail, adding backup systems, or establishing security areas); and

(3) event-mitigating actions, such as establishing shelters, emergency notifications/evacuations, reducing and/or removing inventory quantities, or changing storage locations.

CHAPTER V.

SECURITY AREAS

1. GENERAL REQUIREMENTS. Security areas include property protection areas (PPAs), limited areas, exclusion areas, PAs, vital areas, MAAs, and special designated security areas. The cognizant DOE authority must approve the designation of PPAs.

   a. Prohibited Articles. The following articles are not permitted in a security area without authorization, as established in local procedures. Authorization of prohibited articles to be used for official Government business must be documented in an SSSP or a security plan.

      (1) Explosives.

      (2) Dangerous weapons.

      (3) Instruments or material likely to produce substantial injury to persons or damage to persons or property.

      (4) Controlled substances (e.g., illegal drugs and associated paraphernalia, but not prescription medicine).

      (5) Any other items prohibited by law. Specific information covering prohibited items may be found under the provisions of 10 CFR 860 and 41 CFR 101-20.3.

   b. Controlled Articles. Portable electronic devices capable of recording information or transmitting data (e.g., radio frequency, infrared, and/or data link electronic equipment) are not permitted in limited areas, exclusion areas, PAs, vital areas, and MAAs without authorization. The cognizant DOE authority must approve use of this equipment based on the following criteria: (a) the equipment is mission essential, (b) the equipment is government owned or leased (therefore, involving no additional expense), and (c) a risk analysis identifying vulnerabilities inherent with the characterization and operation of the device has been performed. Authorization for use of such devices in one security area does not apply to all other security areas.

2. SECURITY AREA CONTROL MEASURES. The following requirements apply to security areas other than PPAs.

   a. Access. Access to security areas is controlled to limit entry to cleared and/or authorized individuals.

(1) Any person permitted to enter a security area who does not possess an access authorization at the appropriate level must be escorted at all times by a cleared and knowledgeable individual.

(2) Local authorities must establish escort-to-visitor ratios in a graded manner for each security area.

b. Entry/Exit Inspections. Entry/exit inspections are required at PAs and MAAs, as described in paragraphs 6 and 8 of this chapter, and other security areas identified as required by the cognizant DOE authority and documented in the local SSSP or security plan. Entry inspections of personnel, hand-carried items, packages, and/or vehicles must ensure prohibited articles are detected and prohibited from being introduced into security areas without authorization. Exit inspections must ensure S&S interests are not removed from security areas without authorization. (See Chapter IX of this Manual.)

c. Emergency Personnel and Vehicles. Emergency personnel and vehicles may be authorized immediate entry to security areas in response to an emergency if conditions and procedures for immediate entry are documented in an SSSP or a security plan. Such personnel and vehicles must go through exit inspections when the emergency is over or when leaving the site. If the emergency condition does not permit an exit inspection before site departure, an escort must be provided and both personnel and emergency vehicles must be inspected immediately upon conclusion of the emergency.

d. Signs. Signs prohibiting trespassing must be posted around the perimeter and at each entrance to a security area except when one security area is located within a larger posted security area. Signs must be posted to convey information on the Atomic Weapons and Special Nuclear Materials Rewards Act; prohibited and controlled articles; the inspection of vehicles, packages, hand-carried items, and persons entering or exiting the security area; the use of video surveillance equipment; and trespassing. Chapter XIV of this Manual provides details on posting requirements. (See 42 U.S.C. 2278a Section 229.)

e. Parking Areas.

(1) If parking areas are located near security areas and interference with intrusion detection sensor fields, clear zones, and special response team (SRT) activities could result, these parking issues must be addressed in an SSSP or a security plan.

(2) Vehicle bomb threat must be considered in determining location of vehicle parking areas.

f. Visitor Logs. Visitor logs must be used at PAs, exclusion areas, and MAAs.

(1) Requirements and procedures for visitor logs at security areas must be developed and approved by the cognizant DOE authority. These procedures must provide for recording the following information as a minimum: printed name and signature of the visitor, agency or organization the visitor is representing, visitor's citizenship, person to be visited, purpose of the visit, time of entry, and time of exit. The local authority may establish requirements for additional information.

(2) Automated access control system logs may be used to record visitor information.

(3) Information from visitor registers and logs must be retained in accordance with local records management procedures.

g. Permanent Physical Barriers. These must be used to identify the boundary of a security area. Barriers must achieve the following objectives and meet the requirements described in Chapter X of this Manual.

(1) Barriers should be—

(a) used to direct the flow of personnel and vehicles through designated entry control points;

(b) capable of controlling, impeding, or denying access to a security area;

(c) used to detect and/or deter the introduction of prohibited and controlled articles or the removal of S&S interests; and

(d) used to deter and/or prevent penetration by motorized vehicles where vehicular access could significantly enhance the likelihood of a successful malevolent act.

(2) Penetrations in Security Area Barriers.

(a) Overhead utilities may not pass between security areas without physical protection features to prevent access.

(b) Elevators that penetrate a security area barrier must be provided with an access control system which is equivalent to the access control requirements for the security area penetrated.

(c) Utility corridors that penetrate security area barriers must provide the same degree of penetration resistance as that provided by each barrier they penetrate. This applies when the unattended opening within the utility corridor meets the requirements of paragraph 8b(1) in Chapter X.

(3) Objects that could be used by intruders to scale barriers and enter security areas must not be placed next to barriers.

(4) If a barrier configuration is altered, temporary barriers may be erected (e.g., during construction or transient activities). A vulnerability analysis may have to be conducted that identifies equivalent protection for Departmental assets.

3. PROPERTY PROTECTION AREAS. PPAs are established to protect Government-owned property against damage, destruction, or theft.

a. General Requirements. Protection may include physical barriers, an access control system, protective personnel, IDS alarms, and locks and keys. These protective measures must be described in a security plan and be approved by the cognizant DOE approving authority.

b. Access Control. Access controls may be implemented to protect employees, property, and facilities.

c. Signs Prohibiting Trespassing. Signs prohibiting trespassing must be posted around the perimeter and at each entrance to the PPA. (See Chapter XIV of this Manual.)

d. Inspections. Personnel, vehicles, hand-carried items, and packages entering or exiting the PPA are subject to inspection to deter and/or detect unauthorized introduction of prohibited articles and removal of Government assets.

e. Physical Barriers. Physical barriers such as fences, walls, and doors may be used to identify the boundary of the area.

4. LIMITED AREAS. Limited areas are security areas designated for the protection of classified matter and Category III quantities of SNM.

a. General Requirements. Limited areas are defined by physical barriers encompassing the designated space and access controls to ensure only authorized personnel are allowed to enter and exit the area. Limited area access requirements must be administered as follows.

(1) An individual permitted unescorted access must have an access authorization.

(2) Individuals without appropriate access authorizations or need to know must be escorted, and measures must be taken to prevent compromise of classified matter or access to SNM.

(3) Access to S&S interests within a limited area, when not in approved storage, must be controlled by the custodian or authorized user.

b. Personnel and Vehicle Access Control. The identity and access authorization of each individual allowed access must be validated by protective personnel (e.g., PF or other appropriately authorized personnel), by automated systems, or by other means documented in the SSSP or security plan. Validations must occur at the entry control points to limited areas. Additional access control requirements are as follows.

(1) Non-Government vehicles are prohibited from limited areas unless specifically authorized, in writing, by the cognizant DOE approving authority.

(2) Government owned or leased vehicles may be admitted to limited areas only for official business and only when operated by properly cleared and authorized drivers or when the drivers are escorted by properly cleared and authorized personnel. The cognizant DOE authority must approve procedures for inspection and access of service and delivery vehicles on official business; however, escort by properly cleared and authorized personnel is required.

(3) When a remote automated access control system is used for access control, it must verify the following: a valid DOE security badge (i.e., the badge serial number read by the system must match the serial number assigned to the badge holder) and a valid access authorization. Protective personnel or other means documented in the SSSP or security plan may be used to validate the badge and access authorization at automated entry control points.

5. EXCLUSION AREAS. Exclusion areas are security areas in which an individual's mere presence may result in access to classified matter.

a. General Requirements. The boundaries of exclusion areas must be encompassed by physical barriers. Exclusion areas require access controls that ensure only authorized personnel are allowed to enter and exit the area. Exclusion area requirements are as follows.

(1) Individuals permitted unescorted access must have access authorizations and need to know consistent with the matter to which they would have access by virtue of their presence in the area.

(2) Individuals without access authorization and need-to-know must be escorted, and measures must be taken to prevent compromise of classified matter while these individuals are in the area.

(3) Exclusion areas protecting SNM must provide protection as specified in Chapter II of this Manual.

b. Personnel and Vehicle Access Control. Protective personnel and/or automated systems at entrances must validate the identity and access authorization of persons allowed access. All requirements for personnel and vehicle access control that apply to limited areas also apply to exclusion areas.

6. PROTECTED AREAS. PAs are security areas used to protect Category II quantities or greater of SNM and to provide security zones surrounding separately defined MAAs.

a. General Requirements. PAs must be encompassed by physical barriers identifying their boundaries, surrounded by perimeter intrusion detection and assessment systems (PIDASs), and equipped with access controls that ensure only authorized personnel are allowed to enter and exit. If a PA encompasses an MAA, but no Category II or greater quantities of SNM are present outside the MAA, then at a minimum, random exit inspections must be performed at the PA boundary and documented, with the extent and frequency determined by the cognizant DOE authority.

b. Barriers.

(1) Vehicle barriers must be installed to delay penetrations of the security area.

(2) PA barriers must be designed to detect and/or deter unauthorized access.

(3) The design must also allow for appropriate personnel, vehicle, and materials/packages entry control points while deterring or preventing an insider from passing material over the barrier for later retrieval.

(4) Proximity to buildings or overhanging structures must be considered in barrier design.

(5) The attempted removal of S&S interests by an insider must be a design consideration for site/facility barriers.

c. Entry Control Points. PA entry control point systems must allow for the passage of personnel while detecting the introduction of prohibited and controlled articles. Entry control point design must include separate material package inspection stations so that personnel, packages, and hand-carried items can be inspected. The following criteria apply to the design of entry control points.

(1) Entry/exit point inspection monitors must be colocated with PF posts so that response to an alarm can be initiated expeditiously.

(2) PF posts must be designed with an unobstructed view so that PF personnel can observe any attempt to bypass systems.

d. Protected Area Access. The following requirements apply to PA access.

(1) Entrance inspections of all personnel, vehicles, packages, and hand-carried items must be performed to deter and detect prohibited and controlled articles.

(2) Exit inspections of all vehicles, packages, and hand-carried items must be performed to deter and detect the unauthorized removal of SNM. Specific inspection procedures with limitations and thresholds for SNM and metal detectors must be established and documented.

(a) Exit inspection procedures, detection thresholds for SNM, and shielding must be established consistent with the SNM type, form, quantity, attractiveness level, size, configuration, portability, and credible diversion amounts of SNM contained within the area.

(b) Exit inspections must be capable of detecting shielded SNM (e.g., by using a combination of SNM and metal detectors).

(c) Procedures must ensure that entry control points without the means to detect SNM are not used for an exit except in emergencies.

(3) Exits/entrances must either be alarmed with intrusion detection sensors or controlled at all times.

(4) A PA must be encompassed by a PIDAS. The PIDAS must be monitored in a continuously manned central alarm station (CAS) and secondary alarm station (SAS).

e. Personnel Access Control. The following access control requirements apply.

(1) The identity and access authorization of each person seeking entry must be validated by armed PF personnel and/or by means of an automated access control system.

(2) Where access to a PA is controlled by an unattended automated access control system, the system must verify the following: a valid DOE security badge (i.e., the badge serial number read by the system must match the serial number assigned to the badge holder), valid access authorization, and valid PIN. Protective personnel, or other means documented in the SSSP or security plan, may be used to validate the badge and access authorization at automated entry control points.

f. Vehicle Access Controls. The following requirements apply.

(1) Private vehicles must be prohibited from PAs.

(2) Government owned or leased vehicles or delivery vehicles may be admitted only when on official business and only when operated by properly cleared and authorized drivers or when drivers are escorted by properly cleared, authorized personnel.

7. VITAL AREAS. Vital areas are security areas located within PAs and used for the protection of vital equipment. All vital equipment must be contained within a vital area.

a. General Requirements. In addition to the protection strategies required for PAs, the following must also be used for vital areas.

(1) Area boundaries will conform to the layered protection concept, with a separate vital area perimeter located within a separate and distinct PA.

(2) The perimeter of each vital area must be monitored to deter and detect unauthorized entry attempts.

(3) Vital equipment must be protected with IDSs.

(4) Exits must be alarmed or controlled at all times.

(5) PF response time to an intrusion detection must be less than the delay time that can be demonstrated from alarm activation until the intruders could complete adverse actions.

b. Personnel and Vehicle Access Control.

(1) Validation of the identity and access authorization of persons authorized access must be administered by protective personnel or an automated access control system as determined by the cognizant DOE authority.

(2) Private vehicles must be prohibited from being in a vital area. Government owned or leased vehicles must be admitted only when on official business and when operated by properly cleared and authorized

drivers or when escorted by properly cleared and authorized personnel. Service and delivery vehicles must be admitted only when on authorized business and when driven or escorted properly cleared and authorized personnel.

8. MATERIAL ACCESS AREAS. MAAs are security areas used to protect Category I quantities of SNM or Category II quantities of SNM that roll up to Category I quantities.

a. General Requirements. MAAs must have defined boundaries with barriers that provide sufficient delay time to impede, control, or deter unauthorized access.

(1) MAAs must be located within separate and distinct PAs.

(2) MAA barriers must delay or detect the unauthorized movement of SNM through while allowing access by authorized personnel, material movement through entry control points, and emergency evacuation as necessary. Doors at entry control points, such as transfer locations, must be alarmed and the alarms must communicate with the CAS/SAS when an unauthorized exit occurs.

(3) PF response time to an intrusion alarm must be less than the delay time that can be demonstrated from alarm activation at the PA boundary or before intruders could complete their adverse actions.

(4) Penetrations in the floors, walls, or ceilings for piping, heating, venting, air conditioning, or other support systems must not create accessible paths that could facilitate the removal of S&S interests.

(5) Exits designed for emergency evacuation must be alarmed with intrusion detection sensors or controlled at all times.

b. Entry/Exit Inspections. Inspections must ensure against the unauthorized introduction of prohibited and controlled articles or removal of SNM.

(1) All personnel, vehicles, packages, and hand-carried items must be inspected to detect and prevent the unauthorized introduction of prohibited and controlled articles.

(2) All personnel, vehicles, packages, and hand-carried items must be inspected to detect and prevent the unauthorized removal of SNM and other Government property. Specific inspection procedures and SNM/metal detection thresholds and limitations must be established and documented.

(a) A separate physical or electronic inspection of each vehicle, person, package, and container must be conducted at all exit points for MAAs that contain Category I quantities of SNM.

(b) Exit inspection procedures and detection thresholds for SNM and shielding must be established consistent with the SNM type, form, quantity, attractiveness level, size, configuration, portability, and credible diversion amounts of SNM contained within the area.

(c) Exit inspections must be capable of detecting shielded SNM (e.g., by using a combination of SNM and metal detectors).

c. Personnel and Vehicle Access Control. Access control must be administered by armed PF personnel and/or automated access control systems.

(1) The identity, access authorization, and authority to enter for persons allowed access must be validated at MAA entry control points.

(2) Where access to an MAA is controlled by an unattended automated access control system, the system must verify the following: a valid DOE security badge (i.e., the badge serial number read by the system must match the serial number assigned to the badge holder), valid access authorization, valid biometric template, and valid PIN. Protective personnel, or other means documented in an SSSP or a security plan, may be used to validate the badge and access authorization at automated entry control points.

(3) Private vehicles must be prohibited from MAAs.

(4) Government owned or leased vehicles or delivery vehicles are admitted to MAAs only when on official business. Drivers must have the proper access authorization or be escorted by authorized personnel with the proper access authorization.

9. SPECIAL DESIGNATED SECURITY AREAS. Other areas with restricted access requirements include CASs, SASs, Sensitive Compartmented Information Facilities (SCIFs) and special access program (SAP) facilities, local law enforcement agency or private alarm stations, secure communications centers, and automated information system centers.

a. Special Access Programs. The technical requirements for SAPs are identified in DOE M 471.2-3A, *Special Access Program Policies, Responsibilities, and Procedures,* dated 7-11-02.

b. Alarm Stations. CAS and SAS requirements are described in Chapter VI of this Manual.

c. Sensitive Compartmented Information Facilities. DOE follows the requirements in Director of Central Intelligence Directive 1/21 and DOE "Sensitive Compartmented Information Facility Procedural Guide" for the construction and accreditation of SCIFs.

d. Other Designated Security Alarm Stations. If response by local law enforcement agency/security personnel to alarm activity is permitted, the response must meet the specifications contained in Underwriters Laboratories Inc. Standard 827, "Standard for Central-Station Alarm Services," dated 10-1-96.

e. Secure Communications Centers and Automated Information System Centers.

(1) All centers for handling classified information must be located in a limited area.

(2) Separate access controls and barriers must be established to restrict admittance to persons employed in centers handling classified information or otherwise requiring access to perform their official duties.

(3) Access authorizations, consistent with the highest level and category of classified information handled, must be required for all persons assigned to or having any unescorted access to these centers. A list of persons authorized access must be maintained within the center and a record of all visitors entering the facility must be maintained.

(4) Automated information systems centers and remote interrogation points that process classified information must consider the following.

(a) Control Zone is the inspectable space above, below, and around equipment and distribution systems that is under physical and technical control to preclude interception of compromising emanations.

(b) When contained within a larger limited area, automated information systems centers and remote interrogation points used to process classified information must have separate access controls and barriers.

This page intentionally left blank.

CHAPTER VI.

ALARM MANAGEMENT AND CONTROL SYSTEM

1. GENERAL REQUIREMENTS. This chapter establishes requirements for integrated physical protection systems protecting S&S interests. All IDS alarms used to protect S&S interests must annunciate directly to alarm stations when an alarm device is activated.

   a. Alarm Stations. Alarm stations must provide a capability for monitoring and assessing alarms and initiate responses to S&S incidents.

      (1) Alarm stations must be attended constantly by personnel who possess access authorizations that are commensurate with the most sensitive asset that is under the protection of the alarm station.

      (2) Acknowledgment of alarms must be straightforward and easily performed.

      (3) When closed-circuit television (CCTV) systems are used, the alarm control system must have the capability to call the operators' attention to an alarm-associated video recorder/monitor. The picture quality must allow the operator to recognize and discriminate between human and animal presence in the camera field-of-view.

      (4) Video recorders, when used, must be actuated by alarm signals and operate automatically. The response must be capable of recording an actual intrusion.

      (5) When used as the primary means of alarm assessment and to determine response level, CCTV cameras must have tamper protection and loss-of-video alarm annunciation.

      (6) Access control systems must be used to restrict admittance to persons who require access in the performance of official duties.

      (7) Alarm stations must indicate the status of the systems and annunciate a status change. The system must indicate the type and location of the alarm.

      (8) Records must be kept on each alarm.

b. Alarm Station Architectural Requirements. The alarm station architectural requirements must be of sound construction meeting local building codes.

2. HIGH CONSEQUENCE FACILITIES. Facilities with Category I and II quantities of SNM and other high consequence targets as identified by vulnerability analyses must have a CAS and SAS.

a. CAS and SAS Requirements.

(1) Alarms must annunciate audibly and visibly to both the CAS and SAS simultaneously.

(2) Multiple alarms must be prioritized based on the importance of the S&S interests.

(3) CAS and SAS must be physically separated.

(4) Systems for the protection of Category I and II quantities of SNM installed after July 15, 1994, must use redundant, independently-routed or separate communication paths to avoid a single-point failure.

b. Additional CAS Requirements.

(1) The CAS must meet the requirements of a hardened post and must be located within a limited area.

(2) Exterior walls, windows, doors and roof must be constructed of, or reinforced with, materials that have a bullet-penetration resistance equivalent to the "high-power rifle" Level III rating given in Underwriters Laboratories Inc. Standard 752, "Standard for Bullet-Resisting Equipment," dated 3-10-00.

(3) Personnel entryways must be fitted with doors equipped with locks operable from within the alarm station.

(4) Access to CAS must be limited to authorized personnel only.

c. Additional SAS Requirements. The SAS is an alternative alarm annunciation point that will initiate a response if the CAS cannot perform its intended function. The SAS may be located in a PPA with access to the facility controlled.

3. CLOSED-CIRCUIT TELEVISION SYSTEM. CCTV assessment systems must be functional under day, night, overcast, and artificial lighting conditions. The system must operate in a manner that provides a clear and suitable image for assessment.

   a. Primary Assessment. When CCTV is used for primary assessment, the video subsystem must be integrated with the CAS/SAS alarm display systems. Primary assessment system requirements include the following.

      (1) The system must have the capability to automatically switch to the camera associated with the alarm event and to display that event in the CAS for assessment by the operators.

      (2) Video recorders must be used, be actuated by the intrusion alarm, and record automatically.

      (3) Video recorder response must be rapid enough to record the actual intrusion and be capable of capturing adequate information for alarm assessment.

      (4) Video assessment coverage must be complete with no gaps between zones and no areas that cannot be assessed because of shadows or objects blocking the camera's field of view.

      (5) All cameras must be fixed position, fixed focal length lens when used for assessment. (Pan-tilt-and-zoom cameras may be used for surveillance.)

      (6) CCTV systems must use real-time signal transmission of camera views.

      (7) Manual switching commands must be possible to enable operator-selected views. The video system must accept manual override of automatic features and to permit operation of a CCTV camera associated with another event out of priority order.

   b. Lighting. Sufficient lighting for assessment must be maintained on the PIDAS sensor zones and the clear zone for CCTV assessment and surveillance 24 hours a day.

4. BACKUP POWER SUPPLIES. Backup and emergency power supplies must be provided in accordance with Chapter VIII of this Manual.

This page intentionally left blank.

CHAPTER VII.

PROTECTION OF SECURITY SYSTEMS ELEMENTS

1. GENERAL REQUIREMENTS. Security-related equipment must be protected from unauthorized access in a graded manner consistent with the security interest under protection. System components protecting Government property and security interests other than those itemized must be protected in a manner consistent with a cost/benefit analysis determined by each facility. CASs and SASs must be protected in accordance with Chapter VIII of this Manual. Commercial CASs must be UL Class AA installations. SCIF IDSs follow the requirements of DCID 1/21 and the DOE Sensitive Compartmented Information Facility Procedural Guide.

2. PROTECTIVE FORCE POSTS. The Vulnerability Analysis dictates the location and manning of fixed and mobile posts.

   a. SNM Access. Permanent PF posts controlling access to PAs and MAAs must be constructed to the following requirements for a hardened post. Exterior walls, windows, and doors must be constructed of, or reinforced with, materials that have a bullet-penetration resistance equivalent to the "high-power rifle" rating given in Underwriter Laboratories Inc. Standard 752.

   b. Lighting. Lighting must be capable of providing a minimum of 2 foot-candles luminescence at ground level for at least a 30-foot diameter circle around the post and 0.2 foot-candles for at least 150 feet in all directions.

   c. Vehicular Access Control. Where automated gates are used to control vehicular access to a security area, the gates and openings must be constructed to permit gate operation from inside the post.

   d. PF Towers. If PF towers are to serve as fighting positions, consideration must be given to providing protected firing ports with hardened exterior walls, floors, and windows.

3. INTRUSION DETECTION SYSTEMS. The requirements for physically protecting IDS components are as follows. (See Table 2, Alarm System Protection Requirements.)

   a. Tamper. System components protecting Category I and II quantities of SNM, Top Secret, and vital equipment, must be protected with tamper indication in both the access and the secure modes. Tamper indication is required for intrusion detection/alarm devices, wiring between detection/alarm devices and data-gathering panels (DGPs), and transmission lines from DGPs to annunciators and/or alarm stations.

b. Enclosures and Junction Boxes. Electronic enclosures and junction boxes must be secured against unauthorized access. Manholes and other enclosures, if serving as a junction box for data communication cables, must be protected from unauthorized access.

c. Line Supervision. Line supervision is required for IDSs protecting S&S interests. For PPAs, line supervision may be provided consistent with a cost/benefit analysis determined by each facility. Where data encryption is used, key changes must be made at least annually or whenever compromise is suspected. The requirements for line supervision are listed below.

(1) Line Supervision Options. Different combinations of line supervision are allowed depending on link routing: (a) alarm communication link remaining within the security area or (b) alarm communication link going through a lower security area. Line supervision is required for the two primary segments of alarm data transmission: from sensor to DGPs and from DGPs to DGPs or central processing unit.

(2) Classes of Line Supervision. Performance-based definitions are listed below in descending order of protection.

(a) In general, Classes A through C apply to alarm communication links between DGPs, between DGPs and central alarm computers or alarm annunciator panels, and between computers.

1 For Class A, as a minimum, the data transmission must comply with DOE M 200.1-1, *Telecommunications Security Manual,* dated 3-1-97.

2 For Class B, as a minimum, data must be transmitted by one of the following:

a encryption using a proprietary encryption scheme that results in nonrepetitive communications,

b pseudo-random polling scheme,

c nonencryption over fiber-optic cable enclosed in conduit, or

d nonencryption over fiber-optic cable monitored by an optical supervision system.

3 For Class C, unencrypted data transmissions include the following:

a RS-232, RS-485, etc., data transmissions' standards;

b standard repetitive polling schemes; or

c exception reporting with repetitive polling for health checks.

(b) Classes D through F apply to transmission of information through changes in the analog signal. In general, Classes D through F apply to alarm communication links between a sensor and a DGP.

1 Class D supervision must combine various frequencies of AC, be pulsed DC, or be a combination of AC and DC.

2 Class E supervision must be an AC signal.

3 Class F supervision must be a DC signal.

d. Alarm Annunciation and Response.

(1) Line supervision alarms, Classes A through C, must annunciate in both the CAS and the SAS, indicating the type of alarm (data error, loss of communication, tamper, etc.) and the affected equipment.

(2) Sensor to DGP (Classes C through F) line supervision alarms must annunciate in both the CAS and the SAS, indicating the sensor or sensors affected.

(3) PF personnel must be put on alert and system maintenance personnel notified when line supervision alarms indicate a loss of only one communications path of a redundant system.

(4) Line supervision alarm, tamper alarm, or radio frequency alarm events (e.g., "statement-of-health" alarm, sensor alarm, tamper alarm, and radio frequency jamming indications) must be treated the same as an intrusion alarm for the area being protected.

(5) Maintenance Personnel must be notified of a tamper or line supervision alarm and the alarm condition must be assessed by response force personnel. (See Chapter XIII of this Manual.)

(a) Compensatory measures must be implemented to protect the alarmed location until the required testing and repairs, if applicable, are completed.

(b) Tamper and line supervision alarms must be tested to verify effectiveness, including the capabilities of the alarm system components being protected by the tamper alarm (i.e., BMS, microwave, passive infrared) through physical actuation. (See Table 3.)

Table 2. Alarm System Protection Requirements

SENSOR TO DATA GATHERING PANEL			
Portion of Intrusion Detection System Affected	**Class of Supervision**	**Physical Protection of Alarm Wiring**	**Tamper Switch Wiring Requirements (Cat I & II, TS, vital equipment)**
Data-gathering panel (DGP) to sensor, with DGP located within the area under protection.	Must meet Class F (dc) or higher.	Must meet the requirements of the National Electric Code for protection from damage, per UL-681.	Intrusion detection device tamper switches, must be wired into a 24-hour circuit. It is permissible to wire more than one switch to a circuit if switches are located in the same area. It is permissible to wire tamper switches as part of the line supervision circuit, per UL-681. (See Note 1.)
DGP to sensor, with DGP located outside of the area under protection.	Must meet Class F (dc) supervision with wiring outside of the area being protected installed in a protected manner per UL-681 (See Note 2) or must meet or exceed Class D (complex signal).	Wiring inside of the area under protection must meet the requirements of the National Electric Code for protection from damage, per UL-681. If Class F (dc) supervision is used, then all wiring outside of the area under protection must be protected from access. (See Note 2.)	Intrusion detection device tamper switches must be wired into a 24 hour circuit. It is permissible to wire more than one switch to a circuit if switches are located in the same area. It is permissible to wire tamper switches as part of the line supervision circuit, per UL-681. (See Note 1.)
DATA-GATHERING PANEL TO CENTRAL PROCESSOR CATEGORY I AND II QUANTITIES OF SNM, VITAL EQUIPMENT, AND TOP SECRET CLASSIFIED MATTER			
DGP to central processing unit (CPU) or other computer based systems, with all wiring located within a protected area, material access area, vault, or vault-type room.	Must meet Class C (digital polling) or higher.	Must meet the requirements of the National Electric Code for protection from damage, per ANSI/UL-681.	DGPs and associated equipment must be provided with tamper detection switches, per ANSI/UL-681. (See Note 3.)

Table 2. (continued)

DGP to CPU or other computer based systems, with any of the wiring contained within a property protection area or higher.	Must meet Class B (digital polling) transmitted over fiber optic cable or higher.	Must meet the requirements of the National Electric Code for protection from damage, per UL-681.	DGPs and associated equipment must be provided with tamper detection switches and protected from unauthorized access, per UL-681. (See Note 3.)
DGP to CPU or other computer based systems, with any of the wiring in an unsecured area, allowing unrestricted access to the wiring.	Must meet Class A supervision (DES encryption)	Must meet the requirements of the National Electric Code for protection from damage, per UL-681.	DGPs and associated equipment must be provided with tamper detection switches and protected from unauthorized access, per UL-681. (See Note 3.)

DATA-GATHERING PANEL TO CENTRAL PROCESSOR CATEGORY III AND IV QUANTITIES OF SNM, SECRET AND CONFIDENTIAL CLASSIFIED MATTER

Portion of Intrusion Detection System Affected	Class of Supervision	Physical Protection of Alarm Wiring	Tamper Switch Wiring Requirements
DGP to CPU or other computer based systems.	Must meet Class C (Digital Polling) or higher.	Must meet the requirements of the National Electric Code for protection from damage, per UL-681.	DGPs and associated equipment shall be provided with tamper detection switches and protected from unauthorized access, per UL-681. (See Note 3.)

Notes:

1. Consider wiring tamper switches independent of line supervision circuits for hazardous areas, radiological controlled areas, SNM storage vaults, and other areas where testing and maintenance cost would be offset by the cost of using a separate DGP input for reporting of tamper switches.

2. Acceptable methods for protecting alarm system wiring, where required, are—

   - Using a totally concealed or embedded conduit system.
   - Using threaded conduit [i.e., rigid or intermediate metal conduit (IMC)] for all connections of exposed conduit.
   - Sealing junction boxes, pull boxes, and other openings by welding, epoxy sealed threads, locked cover plates, tamper resistant screws, or tamper alarm switches.
   - Using alarm coverage of all wiring.

3. DGPs and associated equipment must be provided with tamper detection switches on enclosure covers and must be wired into a 24-hour circuit. It is permissible to wire more than one switch to an input if the switches are located in the same general area.

Table 3. Line Supervision Testing

LINK ROUTING	LINE SUPERVISION PROTECTION					
	CATEGORIES I and II SPECIAL NUCLEAR MATERIAL. VITAL EQUIPMENT. SECRET AND ABOVE			CATEGORIES III and IV BELOW SECRET		
	Class	Test (2)	Test (3)	Class	Test (2)	Test (3)
Sensor to Data-Gathering Panel	Manual Testing					
Within Area (1)	E	Weekly	Biweekly	E	Weekly	Biweekly
	B	Monthly	Bimonthly	B	Monthly	Bimonthly
	A	Bimonthly	Quarterly	A	Bimonthly	Quarterly
Through Lower Security Area	B	Weekly	Biweekly	C	Monthly	Bimonthly
	A	Monthly	Bimonthly	A	Quarterly	Semiannually
Through Unsecured Area	A	Weekly	Weekly	B	Monthly	Annually
Data-Gathering Panel to Data-Gathering Panel or Central Processing Unit	Automatic Data Link Integrity Tests					
Within Area (1)	C	60 Minutes		C	60 Minutes	
Through Lower Security Area	B	60 Minutes		C	60 Minutes	
Through Unsecured Area	A	60 Minutes		B	60 Minutes	

(1) Special Nuclear Material, Category I, II - Routing within a Protected Area
(1) Classified - Routing within a Limited Area
(2) Manual Test - No Sensor Self-Test Feature
(3) Manual Test - Sensor Self-Test Feature, with Testing Performed Daily

CHAPTER VIII.

INTRUSION DETECTION AND ASSESSMENT SYSTEMS

1. GENERAL REQUIREMENTS. Intrusion detection and assessment systems used for the protection of SNM, classified matter, and Government property must be installed to ensure breaches of security barriers or boundaries are detected. The systems must be configured so that only authorized personnel may make adjustments.

   a. Protecting SNM. The following requirements apply for alarms protecting Category I and II quantities of SNM.

      (1) Immediate intrusion detection and assessments are mandatory.

      (2) Intrusion detection and assessment systems must function effectively in all environmental conditions and under all types of lighting conditions or compensatory measures must be implemented.

   b. Assessment of IDS Alarms. An effective method must be established for assessing all IDS alarms (e.g., line supervision, intrusion, false, nuisance, system failure, tamper, and radio frequency alarms when radio frequency is used) for the protection of Category I and II quantities of SNM.

      (1) IDS alarms must be assessed immediately by either the PF or CCTV.

      (2) CCTV assessment cameras used as primary assessment for perimeter intrusion detection alarms must be fixed (i.e., not pan and/or tilt).

   c. IDS Monitoring. IDSs must be monitored continuously by CAS/SAS personnel.

   d. Response Capability. Response capability to IDS alarms must be provided to protect S&S interests. Response times must be compatible with the protection strategy employed at the site or as stipulated in Chapter II. The response capability may be provided by assigned protective personnel or by a local law enforcement agency as applicable.

   e. Layered Sensors. The PIDAS must employ multiple detection layers for protecting Category I and II quantities of SNM. Complementary sensor technology is required.

   f. False and Nuisance Alarms. IDSs must be designed, installed, operated, and maintained to ensure that the number of false and nuisance alarms do not reduce system effectiveness.

(1) While maintaining proper detection sensitivity, each interior intrusion detection sensor must have a false alarm rate of less than 1 alarm per 2,400 hours of operation.

(2) While maintaining proper detection sensitivity, each exterior intrusion detection sensor must have a false alarm rate of less than 1 alarm per 24 hours of operation.

(3) If the alarms can be assessed at all times, either visually or by CCTV, a higher false and nuisance alarm rate may be tolerated if such alarms do not degrade the system effectiveness. Even though higher rates may be tolerated, the fact that an alarm occurred must be documented for analysis and trending purposes.

g. Performance. Systems, system components and critical system elements must be performance-tested at a documented frequency in accordance with the requirements of DOE O 470.1. The testing program for systems and system components protecting all other security interests must be developed and implemented in locally-developed security planning documents.

(1) Performance testing must be conducted to validate system effectiveness in providing countermeasures to the design basis threat.

(2) Testing must ensure the line or data link is capable of transmitting an alarm signal and that it has not been compromised.

2. INTERIOR IDS REQUIREMENTS. Interior IDSs are designed to detect unauthorized access to security areas containing classified matter and SNM.

a. Communication Paths. IDSs must be designed with independent redundant data communication paths for protecting Category I and II quantities of SNM.

b. Prevention of Bypass. Interior alarm systems must be designed, installed, and maintained to deter adversaries from circumventing the detection system.

(1) Interior alarms providing protection inside MAAs and vault-type rooms must be installed to eliminate gaps in detection coverage.

(2) The IDS must be tested when it is installed and at least annually thereafter.

(3) If testing indicates degradation of the IDS or any portion thereof, that portion of the IDS must be repaired and retested.

c. Unattended Openings. Interior IDSs may be used as compensatory measures for unattended entry/exit points, utility ducts, or other openings meeting the unattended openings requirements of Chapter X of this Manual.

d. Vault and Vault-Type Room IDS. Vault and vault-type room interior IDS must meet the requirements of Chapter XI of this Manual.

e. BMS IDS. BMSs must initiate an alarm upon attempted substitution of an external magnetic field when the switch is in the normally secured position and whenever the leading edge of the door is moved 1 inch (2.5 centimeters) from the doorjamb.

f. Volumetric Devices. Volumetric interior IDSs must detect an individual moving at a rate of 1 foot per second, or faster, within the total field of view of the sensor and its plane of detection.

g. Performance Testing. Interior IDSs must be functionally tested in accordance with locally established procedures at a documented frequency.

3. EXTERIOR IDS REQUIREMENTS. Exterior IDSs are designed to detect unauthorized entry into security areas.

a. Exterior IDSs must be designed with independent redundant data communications paths for protecting Category I and II quantities of SNM and documented in SSSPs or security plans, consistent with Table 2 of Chapter VII.

b. Detection Capability. A security area PIDAS must be capable of detecting an individual weighing 77 pounds (35 kilograms) or more crossing the detection zone walking, crawling, jumping, running, or rolling at speeds between 1 to 16 feet (0.15 and 5 meters) per second or climbing the fence, if applicable, at any point in the detection zone with a detection probability of 90 percent and at a 95 percent confidence level.

(1) The IDS must be tested when it is installed and at least annually thereafter to validate that it meets detection probability and confidence level requirements.

(2) Any time the IDS falls below the required probability of detection, the IDS must be repaired and retested.

(3) When calculating detection probability for multiple sensor systems, detection is assumed if any of the sensors report an intrusion.

c. Unattended Openings. For all openings in exterior barriers, unattended gates and/or entry/exit points, and culverts and sewers, that meet the unattended opening criteria of Chapter X intrusion detection capabilities must be at least as effective as the rest of the perimeter IDS.

d. Perimeter IDSs must be—

(1) designed to cover the entire perimeter without a gap in detection, including the sides and tops of buildings situated in the detection area;

(2) designed to eliminate areas of detection gaps or no detection. The length of each detection zone must be consistent with the characteristics of the sensors used in that zone and the topography;

(3) designed, installed, and maintained to deter adversaries having the means to circumvent the detection system;

(4) provided with an isolation zone at least 20 feet (6 meters) wide and clear of fabricated or natural objects that would interfere with operation of detection systems or the effectiveness of the assessment; and

(5) free of wires, piping, poles, and similar objects that could be used to assist an intruder traversing the isolation zone or that could assist in the undetected ingress or egress of an adversary or matter. Exceptions to this requirement must be protected by the detection and assessment system or constructed in a manner that deters their use as a means of entering or leaving the area.

e. PIDAS Zones Degradation. Each detection zone of a perimeter IDS must be kept free of snow, ice, grass, weeds, debris, wildlife, and any other item that may degrade effectiveness of the system. When this action cannot be accomplished in a timely manner and detection capabilities become degraded, compensatory measures must be taken to provide timely detection.

4. RADIO FREQUENCY ALARM COMMUNICATIONS. The radio frequency alarm communications systems, when used to protect Category I and II quantities of SNM, must be limited to emergency and temporary situations. The radio frequency communications link that replaces the direct hardwired communications link between the sensor and the CAS display panels must maintain a high level of security.

a. Radio Frequency Alarm Communications Systems. Radio frequency alarm communications systems used for the protection of Category I and II quantities of SNM must, as a minimum, meet the following requirements.

(1) The radio frequency alarm communications system must only be used as one of redundant or alternate paths. A hardwired communications link must be used as the primary method. Using two radio frequencies to protect Category I quantities of SNM—one as the primary and the other as the secondary path—does not meet the requirement for redundant communications paths. An exposed, supervised, hardwired system used

along with radio frequency is adequate as a redundant communication path for temporary applications.

(2) The systems must provide redundant, self-checking alarm communication paths that annunciate system failure in the alarm stations. Alarm messages that are not acknowledged because of a blocked transmission path must be retained as active and communicated later through a status or statement-of-health message.

(3) The statement-of-health interval must allow for an assessment and response.

(4) Radio frequency alarm communication systems must be capable of automatically changing the statement-of-health and alarm messages so the messages are not always the same.

(5) The system must be capable of detecting and annunciating intentional and unintentional radio frequency jamming.

(6) The system must provide unique status change messages for alarm, tamper, and power conditions.

(7) The system must provide random or operator-initiated polling features to ensure communication link integrity.

(8) Digital Encryption Standard encryption or other Government-approved encryption techniques must be used for statement-of-health and alarm messages.

(9) The enclosure must have tamper-resistant or tamper-alarmed transmitters in both the access and secure modes.

(10) The system must have battery backup capabilities.

(11) The system may not produce spurious signals that interfere with other security systems components.

(12) The system must provide a unique electronic address code for each sensor and line supervision from sensor to transmitter.

(13) The system must provide a means of interfacing to the alarm annunciation system (i.e., the CAS).

(14) Compensatory measures must be activated immediately if all or part of the system is being jammed, or if communications are otherwise lost or disrupted. The system must provide communications in all weather conditions and be provided with immediate compensatory measures if communications are lost or degraded. No alarm data may be lost during the period of lost or degraded communications.

(15) The system must ensure system integrity is maintained (i.e., that it is not diminished) during a multiple alarm scenario.

b. Emergency and Temporary Use of Radio Frequency Alarm Communications. Emergency and temporary use of radio frequency alarm communications for the protection of Category I and II quantities of SNM may not exceed 7 days per application and no more than 21 days in a calendar year.

c. Other Requirements. In addition to the above requirements, the site must implement the following procedures for the protection of Category I and II quantities of SNM. Radio frequency alarm communications must—

(1) operate on Government frequency bands;

(2) be installed and maintained using the "two-person" rule;

(3) not change status on a network (e.g., from secure mode to access mode); if the status of the network is changed, the CAS operator must be advised of the mode change; and

(4) be performance tested in accordance with established performance assurance procedures at a documented frequency. (See DOE O 470.1, Chapter III.)

d. Risk Assessment. A risk assessment must be conducted on the radio frequency site system protecting Category I and II quantities of SNM before it is installed to determine system risk to being "spoofed," "bypassed," or "jammed." This assessment must be documented in a report.

5. LIGHTING REQUIREMENTS. Lighting systems must allow detection and assessment of adversaries and reveal unauthorized persons.

a. Protective Lighting—General. Protection system lighting must meet the following criteria.

(1) Illumination must provide for the assessment of unauthorized activities and/or persons at pedestrian and vehicular entrances and allow

examination of identification badges and inspections of personnel, hand-carried items, packages, and vehicles.

(2) Other than at entry control points, lighting must not illuminate patrol paths or PF personnel manning fixed posts. Lighting used to deter adversaries must illuminate outward from the fixed post.

(3) Compensatory measures must be implemented upon lighting system failure.

(4) Lighting must be maintained and tested in accordance with locally approved procedures.

b. Protective Lighting for Category I and II quantities of SNM.

(1) Lights must support a 24-hour visual assessment and, as a minimum, 2–foot-candle illumination at ground level for at least a 30-foot (9.14-meter) diameter around PF posts and within exterior and assessment system isolation zones, and 0.2–foot-candle illumination for 150 feet (45.72 meters) in all directions from within the PA barrier.

(2) Where protective lighting at remote locations is not feasible, PF personnel patrols and/or fixed posts must be equipped with night-vision devices. Night-vision devices must not be used routinely in lieu of protective lighting at entrances and exits but may be used if lighting is lost.

(3) Light glare must be kept to a minimum if it hampers protective personnel.

(4) Light sources on protected perimeters must be located so that illumination is directed outward wherever possible.

6. ELECTRICAL POWER REQUIREMENTS. The requirements for primary and auxiliary power sources are as follows.

a. Primary Power Supply. All IDSs for protecting Category I and II quantities of SNM and Top Secret matter must have a primary power source from normal onsite power. Power sources must contain a switching capability for operational testing to determine adequate auxiliary power sources. The following power supply requirements apply to physical protection systems.

(1) Alarm and Communication Systems. Normal primary power must come directly from the onsite power distribution system or, for isolated facilities, directly from the public utility.

(2) Communications and Automated Information Systems, alarm stations, and radio repeater stations. Critical system elements must be connected to an uninterruptible power supply (UPS) or to auxiliary power.

(3) Radio Control Centers. Power supply requirements must be determined assuming that all transmitters are keyed simultaneously while associated receivers and other equipment and building services are in operation.

b. Auxiliary Power Sources. Intrusion detection and assessment, automated access control, and CCTV systems protecting Category I and II quantities of SNM and Top Secret matter must have an auxiliary power capability.

(1) Transfer to Auxiliary Power must be automatic upon failure of the primary source and not affect operation of the protection system, subcomponents, or devices.

(2) Central Alarm and Secondary Alarm Stations. The CAS and SAS must receive an alarm indicating failure of the protection system's primary power and immediately transfer to the auxiliary power source.

(3) Batteries. Rechargeable batteries, when used, must be kept fully charged, or they must be subject to automatic recharging whenever the voltage drops to a level specified by the battery manufacturer. Nonrechargeable batteries must be replaced whenever their voltage drops 20 percent below the rated voltage or manufacturer's recommendations. An alarm signal must be activated at the CAS and SAS to indicate this condition.

(4) Auxiliary Power Sources must support operational testing and routine maintenance, and be capable of sustaining full operation of auxiliary loads (nominally, a minimum of 8 hours). Such power sources must have the necessary built-in features to facilitate operational testing on a periodic basis to verify their readiness.

c. Uninterruptible Power Sources. A UPS must be provided for those systems requiring continuous power and considered for those systems that, if interrupted, would degrade the protection of the associated security area.

CHAPTER IX.

ACCESS CONTROLS AND ENTRY/EXIT INSPECTIONS

1. GENERAL REQUIREMENTS. The cognizant DOE authority must approve local procedures that implement requirements for access control and entry/exit inspections. The following requirements apply to all security areas except PPAs.

   a. Access to security areas must be controlled.

      (1) Access must be based on an individual's need-to-know in order to perform his/her official duties, validation of the individual's access authorization, and presentation of an approved DOE security badge.

      (2) A person without an appropriate access authorization who is allowed to enter a limited area, exclusion area, PA, vital area or MAA must be escorted at all times by an individual with—

         (a) knowledge of security procedures for those security areas listed above,

         (b) the appropriate access authorization,

         (c) the need-to-know for the security area or for the S&S interests, and

         (d) additional measures that may be needed to prevent compromise of classified matter.

   b. Badge Validation. Access to a DOE security area, as a minimum, requires verification of a valid access authorization and a valid DOE security badge as required by Chapter XV of this Manual.

   c. Layered Access Controls. Access control requirements must be layered in a graded manner at successive boundaries as appropriate for the situation.

   d. Piggybacking. The following requirements must be implemented in the local DOE-approved security plan if "piggybacking" into limited and exclusion areas is permitted at a site. Authorized personnel are permitted to vouch for an individual providing all their access authorization requirements are met.

      (1) Consistent with paragraph (2) below, personnel with the appropriate access authorization may vouch for another person with the required access authorization level to piggyback or enter a limited area that requires a DOE security badge.
      (2) Piggybacking is only allowed in limited areas and exclusion areas.

(3) Authorized personnel permitting piggybacking of another person into a limited area must inspect the individual's DOE security badge to ensure that it bears a likeness of the individual and that he or she has the proper access authorization. Authorized individuals entering a limited area when PF personnel are not controlling access must ensure that unauthorized individuals do not enter (piggyback) into the security area.

(4) Before permitting piggybacking into an exclusion area, need to know must be established.

(5) All personnel within a vehicle are required to produce valid DOE security badges when accessing a limited area.

(6) Sites that allow piggybacking must provide for local implementation procedures and documentation in an SSSP or a security plan.

e. Automated Access Control Systems may be used if the following requirements are met.

(1) Automated access controls, when used for access to any security area, must, as a minimum, verify that the access authorization and the DOE security badge are valid (i.e., that the badge serial number read by the system matches the serial number assigned to the badge holder) as listed in Chapter V of this Manual. Badges must be validated by means of a PIN, when required, or other approved means.

(2) When remote, unattended automated access control system entry control points are used for access to security areas, the barrier must be resistant to bypass without the use of an authorized DOE security badge.

(3) Automated access control system intrusion alarms (e.g., annunciation of a door alarm, duress alarm, tamper alarm, or anti-passback indication feature) must be treated in the same manner as an intrusion alarm for the area being protected.

(a) Both the CAS and SAS must monitor and annunciate the automated access control system's intrusion alarm events used to protect Category I and Category II quantities of SNM.

(b) Electronic entry control point search equipment (e.g., metal detectors) may annunciate locally to an PF-staffed entry control point instead of annunciating at the CAS and SAS.

2. ACCESS CONTROL SYSTEMS AND ENTRY CONTROL POINTS.

a. Positive Controls. Access control systems and entry control points must provide positive control that allows the movement of authorized personnel, vehicles, packages, and hand-carry items along normal routes while detecting and delaying entry of unauthorized personnel, prohibited and controlled articles, and unauthorized removal of S&S interests.

b. Entry Control Point Design. Entry control point designs must incorporate the following.

(1) Entry control points for vehicle and pedestrian access to security areas must provide the same level of protection as that provided at all other points along the security perimeter.

(2) Entry control points must be structurally hardened, as necessary, to meet site-specific criteria.

(3) Exits from security areas must be adequate to satisfy the life safety requirements of National Fire Protection Association (NFPA) 101, "Safety to Life from Fire in Buildings and Structures," dated 2000. Some exits may be provided for emergency use only.

(4) Entrances to and exits from security areas must be equipped with doors, gates, rails, or other movable barriers that direct and control the movement of personnel or vehicles through designated control points.

(5) Door locks and latches used on security area perimeters must meet the requirements of NFPA 101.

(6) Motorized gate controls, where used, must be located within or immediately adjacent to PF posts at entry control points. Motorized gates must be designed to allow manual operation.

(7) Entry control points must facilitate ingress and egress of emergency vehicles and fire protection equipment.

(8) The number of entry control points for each security area must be limited to maintain the barrier integrity.

(9) Where feasible, each entry control point must be placed within the barriers so that the entry control point can be closed during low-traffic periods and the PIDAS enabled. This configuration must provide a continuous PIDAS zone at the barrier that encompasses the entry control point.

c. Entry Control Point Functions. The following functions must be performed at entry control points.

(1) A barrier to personnel entering security areas must be provided until entry is authorized.

(2) Control points used in the protection of SNM must permit entry of only one person at a time.

(3) Access must be controlled whenever a request is made to go from one security area into another security area with increased protection requirements.

(4) Entry and exit inspections must be conducted at entry control points to deter introduction of unauthorized personnel, prohibited and controlled articles, and unauthorized removal of the S&S interest.

3. AUTOMATED ACCESS CONTROL SYSTEMS. Automated access control systems may be used in place of or in conjunction with protective personnel to meet access requirements.

a. Equipment. Automated access control equipment must meet the following requirements.

(1) A DOE security badge must be used to access electronically stored information relevant to the badge and badge holder.

(2) The access authorization list must be updated immediately when an individual's access authorization has changed or when the individual is transferred or reassigned.

(3) Badge readers at PAs and MAAs must have anti-passback protection.

b. Personnel Augmentation of Automated Access Control Systems. Automated access control systems may be used in place of or in conjunction with protective personnel to control access into security areas. If security areas require additional screening (e.g., at a vital area or MAA boundary), and when the PIN or biometric system is either not working or not implemented, PF personnel must be used to validate the use of the DOE security badge as documented in the SSSP or security plan.

c. Protection. Automated access control systems and associated equipment used in the protection of Category I and/or II quantities of SNM, and/or classified matter must be protected in the following manner.

(1) Personnel or other protective measures are required to protect PINs, card reader access transactions, displays (e.g., badge-encoded data), and key pad devices. The process of inputting, storing, displaying, or recording verification data must ensure the data is protected from compromise.

(2) The system must record attempted unsuccessful, unauthorized and authorized access.

(3) Door locks opened by badge readers must be designed to relock immediately after the door has closed.

(4) Transmission lines that carry access authorization and personal identification or verification data between devices/equipment must be protected to deter the introduction of data that would permit unauthorized access.

(5) Access to records and information concerning access authorizations and personal identification or verification data is restricted to individuals cleared at the same level as the information contained within the specific area or areas where identification data or PINs are used. Access to this data, operating system software, or any identifying data associated with the access control system is limited to the least number of people possible consistent within operational requirements.

(6) Records reflecting active assignments of DOE security badges, PINs, levels of access, access authorization, and similar system-related records must be maintained. Records concerning personnel removed from the system must be retained for one year unless a longer period is specified by other requirements.

(7) Badge reader boxes, control lines, and junction boxes must be supervised, tamper-alarmed, or equipped with tamper-resistant devices. DGPs or multiplexers and other similar equipment must be tamper-alarmed or secured by a means that precludes surreptitious tampering with the equipment.

(8) Auxiliary power must be provided at installations where continuous service is required.

4. ENTRY/EXIT INSPECTIONS. The following S&S requirements apply to entry and exit inspections. The inspection process must be documented in the SSSP or security plans and validated.

a. Inspection Program. Protective personnel, in conjunction with inspection equipment when used, such as metal detectors, SNM monitors, explosive detectors, and x-ray systems, must ensure that prohibited and controlled articles are detected before being brought into DOE facilities. Likewise, such programs must ensure S&S interests are not removed. In addition, the following requirements apply.

(1) Passage of individuals, vehicles, and/or packages or mail through entry control point inspection equipment must be observed and controlled by protective personnel. Hand-held and/or portable detectors, etc., must be available to resolve alarms and as compensatory measures for power failures.

(2) Bypass routes around inspection equipment must be closed or monitored to deter unauthorized passage of personnel and hand-carried articles.

(3) Auxiliary power should be provided to all control point inspection equipment.

(4) Measures must be taken to preclude the unauthorized changing of control settings on all entry/exit control point inspection equipment.

(5) Alarms must annunciate audibly and visually to attending protective personnel.

(6) Ingress/egress points must be designed to preclude commingling of searched and unsearched personnel.

b. Entry Inspection Procedures. All personnel, vehicles, packages, and hand-carry articles are subject to inspection prior to or at entrances of security areas to prevent the introduction of unauthorized prohibited and controlled articles.

(1) Explosive Detection.

(a) The SSSP or security plan must document the analysis that establishes the extent to which a facility explosive detection capability provides protection against the malicious use of explosives that could result in an unacceptable risk to public health or safety.

(b) Documentation must include the rationale for explosive detection equipment selection, deployment, and use.

(c) Explosive detection systems, when used, must have a capability of detecting low vapor pressure explosives.

(d) PF procedures for the use of explosive detection equipment must be approved by the cognizant DOE authority.

(2) Metal Detection. Metal detectors used in the inspection process must reasonably ensure weapons are not introduced without authorization.

(a) Metal detectors used for PA entry must, at a minimum, detect test weapons listed in paragraphs 4b(2)(c), 1 and 2 below.

(b) Metal detectors used for MAA entry applications must, at a minimum, detect test weapons listed in paragraphs 4b(2)(c), 1, 2, and 3 below.

(c) The following must be used as standard test weapons:

1 steel and aluminum alloy 0.25-caliber automatic pistol, manufactured in Italy by Armi Tanfoglio Giuseppe, sold in the United States by Excam as Model GT27B and by F.I.E. as the Titan (weight: about 343 grams);

2 aluminum, model 7, 0.380-caliber derringer, manufactured by American Derringer Corporation (weight: about 200 grams); and

3 stainless steel 0.22-caliber long rifle mini-revolver; manufactured by North American Arms (weight: about 129 grams).

(3) X Ray.

(a) X-ray machines are used to reinforce and supplement protective personnel hand searches, for both explosives and metal detectors.

(b) X-ray machines used in the inspection process must be capable of detecting prohibited articles and controlled articles before they are brought into security areas.

(c) X-ray machines must be capable of imaging a 26-gauge wire at Step 5 of an American Society for Testing and Materials (ASTM) step wedge. (See ASTM Standard F792-88.)

(4) SNM Monitors.

(a) SNM monitors must meet detection requirements described in DOE M 474.1-1A.

(b) False alarm rates may not exceed an average of one per 8-hour period.

c. Exit Inspection Procedures. Personnel, vehicles, and hand-carried items, including packages, briefcases, purses, and lunch containers, are subject to exit inspections to deter and detect unauthorized removal of S&S interests from security areas. Collocated SNM monitors and metal detectors must be used at

PAs and/or MAAs to inspect personnel for SNM. Personnel may be inspected visually for classified matter or other S&S interests.

(1) Metal detectors are an acceptable means of inspecting for metallic SNM shielding. When credible theft scenarios do not require the detection of an object (such as lead), and when requirements are properly documented, detection limits suitable to specific situations must be established.

(2) SNM monitors may be used to inspect for concealed SNM.

CHAPTER X.

BARRIERS AND LOCKS

1. GENERAL REQUIREMENTS. Physical barriers, such as fences, walls, and doors, or activated barriers, must be used to deter and delay unauthorized access to security areas. Physical Barriers must serve as the physical demarcation of the security area.

   a. Barriers must be used to facilitate effective and economical use of protective personnel and to direct the flow of personnel and vehicular traffic through designated entry control points to permit efficient operation of access controls and entry point inspections.

   b. Entry control points must provide a barrier resistant to bypass.

   c. Permanent barriers must be used to enclose security areas, except during construction or transient activities, when temporary barriers may be erected. Temporary barriers may be of any height and material that effectively impedes access to the area.

   d. Fences used must be installed not less than 20 feet (6 meters) from the building or material being protected.

   e. Barriers that constitute walls of limited areas used to house security containers for the storage of classified matter must extend from the true floor to the structural ceiling, unless equivalent means are used to provide evidence of penetration of the security area, or access to the security interest being protected.

   f. Wire mesh fencing materials used to enhance penetration resistance must be 2 square inches or smaller mesh of No. 11 American Wire Gauge or heavier steel wire or expanded metal.

   g. Security fences are not required around PPAs.

2. FENCING. When used to protect security areas designated as limited areas or higher, fencing must meet the following minimum construction requirements.

   a. Temporary Security Fencing. During construction or transient activities, temporary security fencing must be installed to—

      (1) exclude unauthorized vehicular and pedestrian traffic from the security area site,
      (2) restrict authorized vehicular traffic to designated access roads, and

(3) provide consistency with site-specific protection goals and operational requirements.

b. Permanent Security Fencing. When permanent fencing is used to enclose limited areas or higher, fencing must meet the following construction requirements.

(1) Alternative barriers may be used instead of fencing if the penetration resistance of the barrier is equal to or greater than security fencing specified in this chapter.

(2) Areas under security fencing subject to water flow, such as bridges, culverts, ditches, and swales, must be blocked with wire or steel bars that adequately provide for the passage of floodwater but also provide a penetration delay equal to that of the security fence.

(3) Depressions where water flow is not a problem must be covered by additional fencing suspended from the lower rail of the main fencing.

(4) Fencing must extend to within 2 inches (5 centimeters) of firm ground, or below the surface if the soil is unstable or subject to erosion. Surfaces must be stabilized in areas where loose sand, shifting soils, or surface waters may cause erosion, thereby assisting an intruder in penetrating the area. Where surface stabilization is impossible or impractical, concrete curbs, sills, or similar type of anchoring device extending below ground level must be provided.

c. Fencing Materials and Specifications. The following requirements apply to fencing materials.

(1) Galvanized steel chain link fabric, consisting of a minimum of 11-gauge with mesh openings not larger than 2 square inches, must be used at security areas. This fencing must be topped by three or more strands of barbed wire on single or double outriggers. Double outriggers may be topped with coiled barbed wire (or with a barbed tape coil). When single barbed wire outriggers are used, they must be angled outward, away from the security area.

(2) Overall fence height, excluding barbed wire or barbed tape coil topping, must be a minimum of 7 feet (2.13 meters).

(3) Wood fencing may be used to comply with nonmagnetic requirements and to obstruct the view.

(4) Fence lines must be kept clear of vegetation, trash, equipment, and other objects that could impede observation or facilitate bridging.

(5) Gate hardware for security fencing must be installed in a manner to mitigate tampering and/or removal (e.g., by brazing, peening, or welding).

(6) A clear zone must be provided along each side of security fences to facilitate intrusion detection and assessment. Double fences should be separated by a clear zone of at least 20 feet (~6 meters). If this minimum distance is not possible, supplementary protective measures must be considered (e.g., greater fence height or other protective measures).

(7) Posts, bracing, and other structural members must be located on the inside of security fences. Where the galvanized finish has been removed or damaged during installation, the posts, bracing, and other structural members must be coated with zinc-enriched paint. (See DOE 6430.1A, *General Design Criteria,* dated 4-6-89.)

(8) Wire ties used to fasten fence fabric to poles must be of equal tensile strength to that of the fence fabric.

3. PERIMETER BARRIER GATES.

a. Motorized Gates. Motorized gates used for entry control points must have the gate controls located within or immediately adjacent to PF posts at each entry control point. Motorized gates must be designed to facilitate manual operation during power outages.

b. Alarm Communications. Primary and auxiliary alarm and communication systems must be provided between entry control points and the response force communications center.

4. WALLS.

a. Barriers. Walls serving as security area boundaries for the protection of classified matter must meet the following requirements.

(1) Building materials must offer penetration resistance to, and evidence of, unauthorized entry into the security area. Construction must meet local building codes.

(2) When transparent glazing material is used, visual access to the classified material must be prevented by the use of drapes, blinds, or other means.

(3) Insert-type panels (if used) must be such that they cannot be removed from outside the area being protected without showing visual evidence of tampering.

b. Exterior Walls. Walls that constitute exterior barriers of security areas must extend from the floor to the structural ceiling, unless equivalent means are used to provide evidence of penetration of the security area, or access to the security interest being protected.

5. CEILINGS AND FLOORS. Ceilings and floors must be constructed of building materials that offer penetration resistance to, and evidence of, unauthorized entry into the area. Construction must meet local building codes.

6. DOORS. Doors, door frames, and doorjambs associated with walls serving as barriers must provide the necessary barrier delay required by the security plan. As a minimum, requirements include the following.

a. Penetration Resistant Doors. Doors with transparent glazing material must offer penetration resistance to and evidence of unauthorized entry into the area.

b. Emergency and Evacuation Exits. Doors that serve exclusively as emergency and evacuation exits from security areas must—

(1) not be accessible from outside the security area,

(2) comply with NFPA 101, and

(3) not open into spaces of greater security.

c. Visual Access. A sight baffle must be used if visual access is a factor.

d. Astragals. An astragal must be used where doors used in pairs meet. Door louvers, baffles, or astragals, when used, must be reinforced and immovable from outside the area being protected.

7. WINDOWS. The following design requirements must be applied to security windows when used as physical barriers.

a. Windows must offer penetration resistance to, and evidence of, unauthorized entry into the area.

b. Frames must be securely anchored in the walls, and windows locked from the inside or installed in fixed (nonoperable) frames so the panes are not removable from outside the area under protection.

c. Visual barriers must be used if visual access is a factor.

8. UNATTENDED OPENINGS.

a. Protection of Unattended Openings. Physical protection features must be implemented at all locations where unattended openings occur, such as where storm sewers, drainage swales, and site utilities intersect the security boundary or area.

b. Criteria. Barriers or alarms are required for all unattended openings for which—

(1) the opening is larger than 96 square inches (619.20 square centimeters) in area and larger than 6 inches (15.24 centimeters) in the smallest dimension and/or the opening is located within 18 feet (5.48 meters) of the ground, roof, or ledge of a lower security area or

(2) the opening is located within 14 feet (4.26 meters) diagonally or directly opposite a window, fire escape, roof, or other opening in an uncontrolled adjacent building or

(3) the opening is not visible from another controlled opening in the same barrier.

9. ACTIVATED BARRIERS, DETERRENTS, AND OBSCURANTS. Activated barriers, deterrents, and obscurants, if used, must meet the following requirements. Obscurants must consider spatial density versus time to deploy as determined by vulnerability analysis. Dispensable materials must be individually evaluated for effectiveness of delay. Controls and dispensers must be protected from tampering and must not be collocated.

10. VEHICLE BARRIERS. Vehicle barriers must be used to preclude, deter, and where necessary, prevent penetration into security areas when such access cannot otherwise be controlled. Sites must have mechanisms in place to ensure the integrity of installed barriers. Above-grade vehicle barriers must be considered to preclude intruder concealment of penetration activities. Speed reducers must be considered to slow adversary vehicles to within vehicle barrier design limits to achieve site-specific threat/target system response requirements consistent with the operational and protection goals of the facility or vulnerability analysis.

11. HARDWARE. Screws, nuts, bolts, hasps, clamps, bars, wire mesh, hinges, and hinge pins must be fastened securely to preclude removal and to ensure visual evidence of tampering. Hardware accessible from outside the security area must be peened, brazed, or spot-welded to preclude removal, or the area must be otherwise secured by use of tamper-resistant hardware (e.g., nonremovable hinge pins).

12. LOCKS. The requirements for security locks must be applied in a graded fashion. Locks used in the protection of classified matter and Category I and II SNM must meet Federal Specifications. (See Federal Specification FF-L-2740A.)

a. Locks used in the protection of classified matter and Categories I and II SNM (e.g., security containers, safes, vaults) must meet Federal Specification FF-L-

2740A "Locks, Combination." This is applicable to locks purchased or installed after the date 7-14-94 and for replacement of damaged equipment.

b. If a combination lock fails on any General Services Administration-approved security container or vault door, it must be repaired or replaced with a lock that meets Federal Specification FF-L-2740A before being used to protect classified matter or Categories I and II SNM.

c. Combination padlocks must meet Federal Specification FF-P-110, "Padlock, Changeable Combination," and standards cited in 41 Code of Federal Regulations Part 101, Federal Property Management Regulations.

d. Key padlocks must meet the following specifications.

(1) High-security, shrouded-shackle, key-operated padlocks must meet standards in Military Specification MIL-P-43607, "Padlock, Key Operated, High Security, Shrouded Shackle."

(2) Key locksets must meet American National Standards Institute Standard A156.2-1996, "Bored and Preassembled Locks and Latches."

(3) Lock bars must be 1-1/4 inch (31.75mm) by 3/16 inch (4.76mm) or equivalent in cross section and constructed of material hardened to Rockwell C59 to C63 standards.

(4) Hasps and yokes on repositories containing classified matter must be constructed of material hardened to Rockwell C59 to C63 standards; be at least 1/4 inch (6.35mm) in diameter or equivalent cross section; and be secured to the repository by welding or riveting.

e. Panic or Emergency Exit Mechanisms. Panic hardware or emergency exit mechanisms used on emergency doors located in security areas must be operable only from inside the perimeter and must meet all applicable Life Safety Codes, as listed in Attachment 3.

f. Key Management. Security keys, key blanks, and key cutting codes, and combinations must be protected at the level as the asset under protection. An inventory and accountability system must be implemented.

CHAPTER XI.

SECURE STORAGE

1. GENERAL REQUIREMENTS. S&S interests must be protected as specified in Chapter II for nuclear weapons and SNM, and Chapter III for classified matter. Secure storage must be in DOE security areas providing security measures equal to or greater than those present in a limited area.

   a. Secure Storage. Vaults, vault-type rooms, or security containers provide secure storage. A vault and/or vault-type room or security container must meet the minimum requirements of a limited area. (See Chapter V of this manual.)

   b. Approved Combination Locks. All security containers placed into service after 7-15-94 must have a lock that meets Federal Specification FF-L-2740A.

   c. Access Controls. Access to vaults and vault-type rooms must be strictly controlled and based on an appropriate access authorization and an authorized need to know. Persons without need to know and the appropriate access authorization must be under escort at all times. Supplementary protective measures to mask classified matter must be used before access by visitors or cleared persons without need to know.

   d. Enhanced Protection. Enhanced verification procedures are required for vaults and vault-type rooms that contain nuclear emergency response assets or nuclear weapons design, use control systems, Sigmas 1, 2, 14, and 15 (see DOE 5610.2, *Control of Weapon Data,* dated 8-1-80, and DOE M 452.4-1, *Protection of Use Control Vulnerabilities and Designs,* dated 7-1-99) or combinations of nuclear weapons design/testing data, and Top Secret or SAP matter.

      (1) Means of controlling access must be documented in an SSSP or a security plan.

      (2) All vaults and vault-type rooms protecting this type of matter must provide for the logging or recording of all personnel entries and exits, including visitors. Logged or recorded entries must include, as a minimum, identification/name and the date and time of entry and exit.

         (a) Automated access controls must log all personnel both in and out of the enhanced protection area. Signatures are not required for automated access control that provide for validation of the DOE security badge, such as use of a PIN, or biometric system.

         (b) Manual logs must be used when automated access controls are not available.

      (3) Other means of controlling access may be used.

e. Miscellaneous Openings. Any miscellaneous openings, of such size and shape to permit unauthorized entry [in excess of 96 square inches (619.20 square centimeters) in an area and more than 6 inches (15.24 centimeters) in its smallest dimension] must be equipped with barriers such as wire mesh, 9-gauge expanded metal, or rigid metal bars at least one-half inch (1.3 centimeters) in diameter, steel, and welded vertically and horizontally 6 inches (15.24 centimeters) on center. The rigid metal bars must be securely fastened at both ends to preclude removal. Where wire mesh, expanded metal, or rigid metal bars are used, care must be exercised to ensure classified matter within the vault cannot be removed with the aid of any type of instrument. After installation, the annular space between the sleeve and the pipe or conduit must be filled with wood, waterproof caulking, or similar material, to give evidence of surreptitious removal.

2. VAULTS AND VAULT-TYPE ROOMS. The minimum standards required for construction of vaults and vault-type rooms, other than GSA-approved modular vaults, apply to all new construction, reconstruction, alterations, modifications, and repairs. The cognizant security office must approve vault-type rooms before they are authorized for storage of classified matter.

a. Vaults. A vault must be a penetration-resistant, windowless enclosure that has doors, walls, floor, and ceiling substantially constructed of materials that afford forced penetration resistance. The material thickness must be determined by the requirement for forcible entry delay times for the S&S interest stored within, but must not be less than the delay time provided by 8-inch (20.32-centimeter) thick reinforced concrete poured in place, with a minimum 28-day compressive strength of 2,500 pounds per square inch (17,237 kilo-Pascal). As an alternative to minimum concrete thickness or structural criteria specified in the following sections, activated barriers may be used to reduce construction and achieve the same delay time.

b. Modular Vaults. A modular vault approved by the GSA may be used in lieu of a vault for the storage of classified matter. The modular vault must be equipped with a GSA-approved vault door and locks, and intrusion detection alarms as specified in paragraph 4b below.

c. Vault-Type Room Construction. The perimeter walls, floors, and ceiling will be permanently constructed and attached to each other. All construction must be done in a manner as to provide visual evidence of unauthorized penetration. The following minimum standards are required for all new construction, reconstruction, alterations, modifications, and repairs of existing areas.

(1) Hardware. Heavy-duty builders' hardware must be used in construction, securely fastened to preclude surreptitious removal and to ensure visual evidence of tampering. Hardware accessible from outside the area must be peened, pinned, brazed, or spot-welded to preclude removal.

(2) Floors and Walls. Construction materials must offer resistance to and evidence of unauthorized entry into the vault-type room. If insert-type panels are used, a method must be devised to prevent the removal of such panels without leaving visual evidence of tampering.

(a) Should any of the outer walls/floors or ceilings be adjacent to space not controlled by DOE, the walls must be constructed of more substantial building materials, such as brick, concrete, corrugated metal, etc.

(b) If visual access is a factor, barrier walls must be opaque or translucent.

(3) Windows. Those windows that open and are less than 18 feet (5.48 meters) from an access point (e.g., another window outside the area, roof, ledge, or door) must be fitted with ½-inch (1.3-centimeter) bars that are separated by no more than 6 inches (15.24 centimeters), plus crossbars to prevent spreading, and/or 18-gauge expanded metal or wire mesh securely fastened on the inside.

(a) If visual access is a security concern, the windows must be closed and locked and made to be translucent or opaque.

(b) During nonworking hours, the windows must be closed and securely fastened to preclude surreptitious entry.

(4) Doors. Doors must be of wood or metal and of substantial construction. Windows, service panels, or similar openings must be secured with 18-gauge expanded metal or wire mesh securely fastened on the inside. Wooden doors must be of solid core construction, 1.75 inches (4.445 centimeters) thick, or faced on the exterior side with at least 16-gauge sheet metal.

(a) If visual access is a security concern, windows must be translucent or opaque.

(b) When doors are used in pairs, an astragal must be installed where the doors meet.

(c) When used, door louvers or baffle plates must be reinforced with 18-gauge expanded metal or wire mesh fastened inside the vault-type room.

(5) Ceilings.

(a) When barrier walls do not extend to the true ceiling and if a false ceiling is created, the false ceiling must be reinforced with 18-gauge expanded metal or wire mesh to serve as a true ceiling or ceiling tile clips must be secured.

1 Any wire mesh or expanded metal used must overlap the adjoining walls and be secured to show evidence of any tampering.

2 When ceiling tile clips are used, a minimum of four clips must be installed per tile. The clips must be installed from the interior of the area, and each clip must be mounted to preclude surreptitious entry.

(b) In some instances, it may not be practical to erect a solid suspended ceiling as part of the vault-type room. For example, in vault-type rooms where overhead cranes are used to move bulky equipment, the air-conditioning system may be impeded by the construction of a solid suspended ceiling, or the height of the classified matter may make a suspended ceiling impractical. In such cases, special provisions, such as motion detection systems, must be used to ensure that the area cannot be entered surreptitiously by going over the top of the walls.

3. VAULT-TYPE ROOM COMPLEX. Vault-type room complex barriers must meet the penetration resistance, intrusion detection, and access control requirements in order to be used for open storage of classified matter.

a. Vault-Type Room Criteria. Vault-type room S&S criteria may be extended to multiple rooms, including an entire building. Protective measures must ensure that the security interest is surrounded by an IDS alarm or that the entire surrounding perimeter is able to detect penetration. Individuals must be authorized for access to all S&S interests within the vault-type room complex before they are allowed to enter, or supplementary protective measures to shield the security interest from view must be employed.

b. Vault-Type Room Complex General Requirements. The general requirements for a vault-type room complex are listed below.

(1) Barrier requirements apply to the outer walls, floor, and ceiling.

(2) Outer walls must extend from true floor to true ceiling.
(3) Interior walls may extend only to a false ceiling and/or raised floor.

(4) Interior doors, windows, and openings may exist between different work areas.

(5) Access authorization and need-to-know restrictions must be enforced.

c. Detection of Unauthorized Access. The requirement to detect unauthorized access may be accomplished through direct visual observation by an individual authorized in the area or through intrusion detection sensors. Detection of inner wall penetration or motion within the vault-type room complex is required. False ceilings and raised floors are permitted.

d. IDS Sensors. Intrusion detection sensors associated with walls, floors, and ceilings that are not under constant visual surveillance but are associated with the vault-type room complex must be activated and functioning at all times.

4. INTRUSION DETECTION SYSTEMS. IDSs are required for vaults, vault-type rooms, and in some instances containers, used to store classified matter.

a. Vaults. Doors or openings allowing access into vaults must be equipped with IDS devices. A BMS, or other equally effective device, must be used on each door or movable opening to allow detection of attempted or actual unauthorized access.

b. Vault-Type Rooms. IDSs must be capable of detecting penetration through floors, walls, ceilings, and openings, or movement within the vault-type rooms, consistent with that required to remove or compromise S&S interests.

(1) Where IDS sensors are used to detect vault-type room envelope penetration, the unattended openings discussed in paragraph 8 of Chapter X must also be protected.

(2) Where IDS sensors are used to detect movement within the vault-type room, sensor coverage must be provided for credible pathways from the exterior barrier to the matter being protected. If the distance between the true floor (or ceilings) and the false floor (or ceilings) exceed 6 inches (15.24 centimeters), intrusion alarms are required between the two floors (or ceilings).

(3) In addition to detecting penetration of the vault-type room or movement in the room, a BMS or other effective device must be used on each door or movable opening to allow detection of attempted or actual unauthorized access.

5. SECURITY CABINETS/CONTAINERS. The GSA establishes the national minimum standards and specifications for commercially manufactured security containers or

cabinets. Containers purchased after 7-14-94 must conform to the latest GSA standards and specifications.

a. Security Cabinets/Containers Requirements.

(1) Label and Mark. Security containers, cabinets, or repositories must bear a test certification label on the inside of the locking drawer or door and must be marked "GSA-Approved Security Container" on the outside of the top drawer or door.

(2) Maintenance. A history for each security container describing damage sustained and repairs accomplished must be recorded on Optional Form 89 and retained for the life of the security container.

(3) Transfer of Security Containers. When a security container is transferred from one organization to another, the custodian from the original organization must certify in writing that all classified matter has been removed before the transfer takes place. Certification must be made to the organization's security office and must include the security container's make and property tag number (or other unique identifying numbers or markings), the custodian's name and organization, and the statement "All classified matter was removed from this (these) security container(s) before transfer from (transferring organization) to (receiving organization)."

b. Damage and Repair of GSA-Approved Security Containers. Only cleared or escorted safe technicians or locksmiths may neutralize lock-outs or repair any damage that affects the integrity of a security container approved for the storage of classified information.

(1) Requirements in FED-STD-809, must be met for neutralization and repair of GSA-approved containers and vault doors.

(2) Physically modified containers are not considered approved by GSA.

CHAPTER XII.

COMMUNICATIONS

1. GENERAL REQUIREMENTS. Communications equipment must be provided to facilitate reliable information exchanges between protective personnel. The communications equipment must meet the following requirements.

   a. Redundant Voice Communications. Facilities protecting Category I and II quantities of SNM must have a minimum of two different voice communications technologies to link the CAS/SAS to each fixed post and PF personnel dispatch station within the facility.

      (1) Alternate communications capabilities must be available immediately upon failure of the primary communications system. Channels considered critical to protective personnel communications must have backup stations.

      (2) Records of the failure and repair of all communications equipment must be maintained in a form suitable for compilation by type of failure, unit serial number, and equipment type.

   b. Recording of Communication. A continuous electronic recording system must be provided for all security radio traffic and telecommunications lines that provide support to the CASs. The recorder must be equipped with a time track and must cover all security channels. This recording requires the approval of the Office of Chief Information Officer or the Office of Security. (See DOE 1450.4, *Consensual Listening-In To or Recording Telephone/Radio Conversations,* dated 11-12-92.)

   c. Loss of Primary Power. Systems must remain operable during the loss and recovery of primary electrical power.

2. COMMUNICATION SYSTEMS. Protection system communications must support two vital functions: alarm communication/display and PF communications. Chapter VI, Alarm Management and Control System, describes the established requirements. PF communications include the procedures and hardware that allow members to communicate with each other.

   a. Design Considerations. The design of a PF communication system must address specific features, resistance to eavesdropping, vulnerability to transmission of deceptive messages, and susceptibility to jamming.

   b. Special Response Team Requirements. SRT members must use two-way radios equipped with digital encryption that complies with DOE M 200.1-1. SRT radio

communications equipment must function as part of the PF radio system, be capable of transmitting routine and emergency information, and use channels that are separate from the normal operations channels.

c. Alternate Means of Communication. Alternate means of communication must be in place, such as telephones, intercoms, public address systems, hand signals, sirens, lights, pagers, couriers, computer terminals, flares, duress alarms, smoke, or whistles.

d. Local Law Enforcement Agency Enforcement. CASs (and PF secure communications center) must be equipped with radio and telephone channels for communication with local law enforcement agencies. An alternative communications capability from a SAS must be provided for use if the primary station is compromised.

3. DURESS SYSTEMS. Facilities with PAs, MAAs, and vital areas must have duress notification capabilities for mobile and fixed posts, and for the CAS/SAS. The duress system must meet the following requirements.

a. Activation of the duress alarm must be as unobtrusive as practicable. The duress alarm must annunciate at the CAS and SAS, but not at the initiating PF post.

b. The duress alarm for a CAS must annunciate at the SAS, while the duress alarm for the SAS must annunciate at the CAS.

c. Mobile duress alarms must annunciate at the CAS, SAS, or another fixed post.

4. RADIOS. Fixed post radios, mobile radios, and portable radios must be provided to support operational security requirements and the security police officer (SPO) SRT-SPO III requirements.

a. Radio System Requirements. The radio system must be capable of accessing security operational and support channels.

(1) The radios must have sufficient power and sensitivity for two-way voice communications with the facility base stations using the primary channel.

(2) Security communication channels must be restricted to security operations.

b. Portable Radios.

(1) Portable radios must be capable of two-way communication on the primary security channel from within buildings and structures.

(2) An alternate means of communications must be provided if safety or process procedures prohibit transmission within a building or structure.

c. Two-Way Communications. Mobile radios and base station radios must be capable of maintaining two-way communication with the CAS/SAS on the primary channel.

d. Emergency Response Channels. Base stations, which are controlled from the CAS, must include emergency response channels.

e. Battery Power. Portable radios must contain sufficient battery capacity to operate for an eight-hour period at maximum expected duty cycles. Procedures for radio exchange, battery exchange, or battery recharges can be used to meet this requirement.

f. Repeater Stations. A radio repeater station must be placed in a location that ensures all-weather access for vehicles and personnel to the station building, antenna, standby generator plant, and fuel storage tanks. The station must be designed to minimize risk of damage to the antenna structure and supporting guy lines from vehicular traffic.

This page intentionally left blank.

CHAPTER XIII.

MAINTENANCE

1. GENERAL REQUIREMENTS. Security-related subsystems and components must be maintained in operable condition. System maintenance must be applied in a graded fashion. A regularly scheduled testing and maintenance program must be established and documented.

2. CORRECTIVE MAINTENANCE. Corrective maintenance must be performed on site-determined critical and noncritical physical protection system elements. (See DOE O 470.1, Chapter III.)

   a. Compensatory Measures. Compensatory measures must be implemented immediately when any part of the critical system element protecting Category I and II quantities of SNM, vital equipment, and Top Secret matter is out of service. Compensatory measures must be continued until maintenance is complete and the critical system element is back in service. For noncritical system elements, the cognizant DOE authority must approve compensatory measure procedures.

   b. Corrective Maintenance for Category I and II SNM. Corrective maintenance must be initiated within 24 hours of the indication that a malfunction of a site-determined critical system element has occurred for systems protecting Category I and II quantities of SNM, vital equipment, and Top Secret matter.

   c. Corrective Maintenance Within 72 Hours. Corrective maintenance must be initiated within 72 hours of detection of a malfunction for all other protection system elements protecting Category I and II SNM, vital equipment, and Top Secret matter.

   d. Other Corrective Maintenance. Corrective maintenance procedures for protecting Category III and IV quantities of SNM and Secret and Confidential matter must be approved by the cognizant DOE approving authority and prescribed in the site's operation procedures.

3. PREVENTIVE MAINTENANCE. Preventive maintenance must be performed on critical S&S-related subsystems and components. Preventive maintenance must comply, at a minimum, with manufacturer's specifications and recommendations.

   a. Critical Component Preventive Maintenance. The following system elements must be included in a preventive maintenance program:

      (1) intrusion detection and assessment systems,

      (2) CAS and SAS communications and display systems,

(3) data and voice communications systems,

(4) PF equipment,

(5) access control and entry/exit inspection equipment,

(6) package and hand-carry items inspection equipment,

(7) vehicle access control and inspection equipment, and

(8) security and safety lighting systems.

b. Other Preventative Maintenance. The PIDAS, security area and other security lighting, and security system-related emergency power or auxiliary power supplies must be included in a preventative maintenance program.

4. MAINTENANCE PERSONNEL ACCESS AUTHORIZATION. Personnel who test, maintain, or service critical system elements must have access authorizations consistent with the category of SNM and/or classified matter being protected. Access authorizations are not required when such testing and maintenance are performed as bench services away from the security area or are performed under the supervision of an appropriately cleared custodian knowledgeable of the system and/or critical system element. Systems or critical system elements bench-tested or maintained away from a security area by personnel without the appropriate access authorizations must be inspected and operationally tested by qualified and cleared personnel before being returned to service.

5. RECORD KEEPING. Testing and maintenance records must be retained in accordance with the requirements of locally approved records management procedures.

CHAPTER XIV.

POSTING NOTICES

1. GENERAL REQUIREMENTS. Signs must be posted at facilities, installations, and real property based on the need to implement Federal statutes protecting against degradation of S&S interests.

   a. Signs. Signs listing prohibited and controlled articles, as stated in paragraph 1a. of Chapter V, must be posted at entrances to security areas.

   b. Warning Signs. Warning signs and/or notices must be posted at entrances to areas under electronic surveillance protection advising that physical protection surveillance equipment is operating.

2. TRESPASSING. DOE property must be posted according to statutes, regulations, and the administrative requirements for posting specified in this Manual.

   a. Statutory and Regulatory Provisions.

      (1) Section 229 of the Atomic Energy Act of 1954, as amended, (42 U.S.C. 2278a) and as implemented by 10 CFR 860, prohibits unauthorized entry and unauthorized carrying, transporting, or otherwise introducing or causing to be introduced any dangerous weapon, explosives, or other dangerous instrument or matter likely to produce substantial injury to persons or damage to property into or upon any facility, installation, or real property subject to the jurisdiction, administration, or in the custody of DOE. The statute provides for the posting regulations and penalties for violations.

      (2) Section 662 of the Department of Energy Organization Act (42 U.S.C. 7270b), as implemented by 10 CFR 1048, prohibits unauthorized entry upon and unauthorized carrying, transporting, or otherwise introducing or causing to be introduced, any dangerous instrument or material likely to produce substantial injury to persons or damage to property into or onto the Strategic Petroleum Reserve, its storage or related facilities, or real property subject to the jurisdiction, administration, or custody of DOE. The statute provides for posting the regulations and penalties for violations.

      (3) Title 41 CFR 101-19.3 provides rules and regulations governing entry to public buildings and grounds under the charge and control of GSA.

b. Posting Proposals. Requirements for the administration of posting proposals are as follows.

(1) Conditions. Proposals for the posting of facilities, installations, or real property, or amendment to or revocation of a previous proposal, must be submitted when one of the following occurs.

(a) The property is owned by or contracted to the United States for DOE use.

(b) The property requires protection under Section 229, Atomic Energy Act of 1954, as amended, and/or Section 662 of the Department of Energy Organization Act. (See 42 U.S.C. 7101, Section 662.)

(c) A previous notice needs to be amended or revoked.

(2) Contents.

(a) Each posting proposal must contain the name and specific location of the installation, facility, or real property to be covered and the boundary coordinates. If boundary coordinates are not available, the proposal must include a description that will furnish reasonable notice of the area to be covered, which may be an entire area or any portion thereof that can be physically delineated by the posting indicated in paragraph 2c below.

(b) Each proposal for amendment or revocation must identify the property involved, state clearly the action to be taken (i.e., change in property description, correction, or revocation), and contain a new or revised property description, if required.

c. Posting Requirements.

(1) Upon approval by the Office of Security, a notice designating the facility, installation, or real property subject to the jurisdiction or administration, or in the custody of, DOE must be published in the *Federal Register*. The notice is effective upon such publication, providing the notices stating the pertinent prohibitions and penalties are posted. (See 10 CFR 860.7.)

(2) Property approved by the Office of Security must be posted at entrances and at such intervals along the perimeter of the property to ensure notification of persons about to enter. Signs must measure at least 11 inches by 14 inches (28 by 36 centimeters).

d. Notification to the Federal Bureau of Investigation. Notification of the date of posting, relocation, removal of posting, or other change, and the identity of the property involved, must be furnished to the applicable office of the FBI exercising investigative responsibility over the property.

This page intentionally left blank.

CHAPTER XV.

DOE BADGE PROGRAM

1. GENERAL REQUIREMENTS. The DOE security badge or the Office of Science badge is the only format to be used.

   a. DOE Security Badge. DOE security badges must be issued to and worn by all DOE and contractor personnel to gain access to DOE contractor-operated facilities with S&S interests, and/or security areas. In addition, the following requirements apply.

      (1) Specifications for the DOE security badge as set forth in Attachment 4.

      (2) The DOE security badge will be accepted at all DOE facilities, including those facilities where the Office of Science badge is issued. Individuals with an access authorization at Office of Science facilities must be issued a DOE security badge to gain access to other non-Office of Science DOE facilities.

         (a) Local Site-Specific Only (LSSO) Badges. LSSO badge requirements are described in Attachment 4.

         (b) Employee identification cards must not be substituted for the DOE security badge or the Office of Science badge.

         (c) The Office of Science issued badge is not authorized for access to DOE facilities that require the DOE security badge.

   b. Office of Science Badge. The Office of Science must prepare and distribute specifications for the badge. The cognizant DOE authority must approve locally developed procedures for the issuance, use, recovery, accountability, protection and destruction of the Office of Science badge that are documented in the security plan. Facilities operated exclusively by the Office of Science, Office of Fossil Energy, and the Office of Energy Efficiency and Renewable Energy that use the Office of Science badge are exempted from the DOE security badge requirements.

2. DOE SECURITY BADGES. Facilities that use the Office of Science badge are exempted from the remainder of the DOE security badge requirements in this chapter. DOE security badge categories are as follows.

   a. DOE Federal and Contractor Employee Badges. These are the permanent DOE security badges that must be issued to DOE and contractor employees for access to sites throughout the DOE complex.

(1) Only one permanent DOE security badge may be issued to each employee.

(2) These badges must be issued by the organization/badging authority reporting to the DOE element maintaining the badge holder's master personnel clearance files.

b. LSSO Badges. LSSO badges may be developed and issued to address a variety of issues and unique local badging requirements.

(1) LSSO badges include visitor badges, vendor badges, provisional badges, foreign national (FN) badges, and other site-specific badges designed and implemented to meet local requirements.

(a) LSSO badges must follow local design guides and must not resemble the design of the DOE security badges.

(b) Non-Federal, delivery, service and maintenance personnel whose duties require regular or routine access to Departmental facilities may be issued an LSSO badge or other site-specific badge. Site access for this category of personnel must follow procedures as approved by the cognizant DOE approving authority.

(2) The cognizant DOE approving authority must prescribe procedures for the design, issuance, use, accountability, and return of LSSO badges.

(a) The issuing authority must instruct the recipient that LSSO badges will only be used at the issuing site, as well as any other site limitations that may apply.

(b) Sites may not grant access to anyone using an LSSO badge issued by another site.

(c) LSSO badges issued by other than the local DOE approving authority and used in an attempt to gain access must be confiscated.

(d) The LSSO badge may or may not contain the individual's photograph.

(3) LSSO temporary and visitor badges are allowed to use the color coding for access authorization and be usable in the site's automated access controls system. However, LSSO temporary and visitor badges must be distinctive in other ways to prevent their use at sites other than the site where the badges were issued.

c. Visitor Badges. A procedure for the issuance of visitor badges must be locally implemented. The visited site must issue an LSSO badge for the onsite visit of authorized personnel who have not been provided a DOE security badge.

(1) An LSSO badge may be issued to visitors, such as military and other Federal agency personnel who require long-term access to DOE facilities but do not occupy full-time DOE positions.

(2) Cleared visitors may be issued an LSSO badge if they possess a "Q" or "L" DOE access authorization or a "TS" or "S" clearance granted by another Federal agency. This category includes—

(a) DOE contractors, military, and other Federal personnel who are given site-specific access but whose duties do not require them to access other DOE facilities and

(b) those personnel possessing a "TS" or "S" clearance and awaiting a final DOE Q or L access authorization.

(3) Visitors and military or other Federal agency personnel not provided with permanent DOE security badges must follow the visitation procedures of the site to be visited as approved by the cognizant DOE approving authority.

(4) Individuals who have been issued an LSSO badge and who want to visit another site and need access to limited areas, exclusion areas, PAs, and MAAs or classified information, must submit DOE F 5631.20, "Request for Visit or Access Approval." (See DOE O 470.1, Chapter VIII.)

(a) The request must be submitted by the individual's DOE sponsor if he/she travels in the Government's interest or by the individual's parent employer if he/she travels in the employer's interest.

(b) Visit requests must be sent directly from visiting individuals' security officer to the security officer at the sites to be visited.

d. Temporary Badges. Temporary badges may be issued to DOE and DOE contractor employees under the locally developed procedures as a interim measure when badges are lost, forgotten, or stolen. Temporary badges may be designed without the use of the DOE security badge color coding indicating an access authorization, and without the name and photograph. Temporary badges must clearly indicate the temporary nature of the badge.

e. FN Badges. Badges issued to FNs must be as follows.

(1) Cleared FNs must be issued a DOE security badge. The difference between the cleared FNs badge and the DOE security badge is that the individual's country of citizenship must be displayed. The DOE security badge issued to a cleared FN must be issued by the organization/badging authority reporting to the DOE element holding the FNs personnel clearance file. Cleared FNs must adhere to the requirements in DOE N 142.1, *Unclassified Foreign Visits and Assignments,* dated 7-14-99, or Chapter VIII of DOE O 470.1, when visiting other DOE facilities.

(2) Uncleared Foreign Nationals. An LSSO badge must be issued to uncleared employees who are not citizens of the United States and whose official duties require routine or regular access to DOE facilities. These badges issued to uncleared FN employees must be red in color. Note: The color red is reserved exclusively for uncleared FN badges. This color must not be used for any other type of LSSO badge.

3. ISSUANCE, USE, RECOVERY, AND DESTRUCTION OF DOE SECURITY BADGES.

a. Issuance of DOE Security Badges. DOE security badges must be issued to all DOE and contractor employees who have been granted access authorizations. These badges must be used and accepted at all other sites and facilities. (See DOE O 472.1B.)

b. Site Usage. A DOE security badge must be used and accepted as evidence of an access authorization and must be accepted for admittance to security areas without need for additional security badging.

(1) The organization being visited is responsible for verifying an individual's DOE access authorization level and determining need to know before granting access to SNM or classified information.

(2) The information on the magnetic stripe must not be used for any purpose other than access control. The information on the magnetic stripe must not be collected or stored outside of DOE access control applications.

c. Individual Requirements. The cognizant DOE authority must approve implementing procedures to ensure individuals receiving the DOE security badge are responsible for the following:

(1) protecting the security badge against loss, theft, or misuse and reporting a lost, stolen, or misused badge to the cognizant security office within 24 hours of discovery;

(2) maintaining the DOE security badge in good condition and protecting its integrity by ensuring that the badge is not altered, photocopied, counterfeited, reproduced, or photographed;

(3) returning the DOE security badge according to local procedures as approved by the cognizant DOE authority when it is no longer valid or required;

(4) surrendering or returning the DOE security badge when requested according to local procedures approved the cognizant DOE authority;

(5) wearing the DOE security badge conspicuously, photo side out, in a location above the waist and on the front of the body while having access to DOE facilities (a deviation to this requirement may be permitted for health or safety reasons); and

(6) not using the DOE security badge outside of DOE facilities for other than Government purposes.

d. Thirty-Person-or-Less Operations.

(1) DOE security badges must be used at DOE and contractor facilities and operations involving access of 30 or more people.

(2) Facilities and operations involving access of less than 30 people may be excluded from the DOE security badge requirement only when the nature of activities and involvements permits adherence to a personal recognition system that provides similarly high levels of assurance that unauthorized persons will not be allowed access to security areas, facilities, classified matter, or other security interests.

e. Recovery of DOE Security Badges. DOE security badges are the property of the Government. Local procedures must be established for returning security badges to the issuing office whenever an individual has terminated employment, is transferred (including transfer of contractor between contracts and when changing employment with contractors at the same site), or otherwise no longer requires the badge.

(1) Individuals who no longer have a valid requirement for access to DOE facilities must surrender their badges according to local procedures as approved by the cognizant DOE authority.

(2) Badges issued to employees, contractors, and other individuals must be recovered at the final security checkpoint or earlier, and the individuals

must be escorted from the site if circumstances or conditions indicate such action is needed. Recovered DOE security badges must be destroyed.

(3) If a terminated employee's DOE security badge is not recovered, the badge must be treated as a lost or stolen badge and immediately reported to the issuing office.

f. Individual Changes of Appearance. A DOE security badge may be confiscated and reissued, with a new photograph, if the individual's appearance has changed significantly.

g. Badge Destruction. DOE security badges that are no longer needed must be destroyed so that the badge cannot be reconstructed. If destruction is not immediate, badges must be stored in a secure manner until they can be destroyed. Temporary and visitor's badges that do not include individuals' photos must be recovered and may be reissued.

4. ACCOUNTABILITY OF DOE SECURITY BADGES. Records must be maintained by issuing offices showing the disposition of DOE security badges. Such records must include, as a minimum, the description and serial number; date of issuance; and name, organization, and date of destruction.

a. Records. Records must be maintained in accordance with the requirements of the local records management program.

b. Lost Badges. A record of missing DOE security badges must be maintained. Personnel and/or systems controlling access to DOE security areas must be provided current information regarding missing badges to prevent badge misuse. The loss or recovery of DOE security badges must be reported immediately to the issuing office.

5. PROTECTION OF DOE SECURITY BADGE MATERIALS AND EQUIPMENT. Stocks of badging materials, unissued DOE security badges, and badge-making and processing equipment must be stored to protect against loss, theft, or unauthorized use.

6. DOE SECURITY BADGE VALIDATION. The cognizant DOE authority must approve local procedures for validation of the DOE security badge at access control points (e.g., automation or PF physical examination of the security badge). Procedures must require PF or assigned security personnel to validate the DOE security badge at all DOE facilities including those worn by pedestrians or vehicle occupants, and to ensure that the badge photo matches the presenter's face and that the badge has not been altered.

a. Badge validation by PF or security personnel is not required at access control points that rely on automated access control systems for entry into DOE facilities.
b. Other methods of validation may be instituted as specified in Chapter IX.

7. DOE SECURITY BADGE SPECIFICATIONS. The DOE Security Badge Specifications are described in Attachment 4. An appendix to the attachment identifying the specific details of the security badge is marked "OFFICIAL USE ONLY" and will be issued separately from the manual. A copy of the DOE Security Badge Specifications may be obtained by contacting the program manager of Protection Program Operations at 301-903-6209.

This page intentionally left blank.

Department of Energy Elements to Which DOE M 473.1-1,
Physical Protection Program Manual, **Is Applicable**

Office of the Secretary

Office of the Chief Information Officer

Office of Civilian Radioactive Waste Management

Office of Congressional and Intergovernmental Affairs

Office of Counterintelligence

Departmental Representative to the Defense Nuclear Facilities Safety Board

Office of Economic Impact and Diversity

Office of Energy Efficiency and Renewable Energy

Energy Information Administration

Office of Environment, Safety and Health

Office of Environmental Management

Office of Fossil Energy

Office of General Counsel

Office of Hearings and Appeals

Office of Independent Oversight and Performance Assurance

Office of the Inspector General

Office of Intelligence

Office of Management, Budget and Evaluation and Chief Financial Officer

National Nuclear Security Administration

Office of Nuclear Energy, Science and Technology

Office of Policy and International Affairs

Office of Public Affairs

Office of Science

Secretary of Energy Advisory Board

Office of Security

Office of Worker and Community Transition

Office of Energy Assurance

Bonneville Power Administration

Southeastern Power Administration

Southwestern Power Administration

Western Area Power Administration

CONTRACTOR REQUIREMENTS DOCUMENT

DOE M 473.1-1, *Physical Protection Program Manual*

All requirements contained in DOE M 473.1-1, *Physical Protection Program Manual,* dated XX-XX-02, apply to contractors who are responsible for operating and/or administering the Department of Energy (DOE), including the National Nuclear Security Administration, physical protection program and/or for protecting safeguards and security (S&S) interests. The requirements in DOE M 473.1-1 must be assigned to all subcontractors who have responsibilities for operating, administering, and/or protecting DOE S&S interests.

REFERENCES

1. Title 42 United States Code (U.S.C.) 7270b, Trespass on Strategic Petroleum Reserve Facilities, authorizes issuance of regulations concerning unauthorized entry into or upon the Strategic Petroleum Reserve, its storage or related facilities, or real property subject to the jurisdiction, administration, or in the custody of the Secretary of Energy under Part B of Title I of the Energy Policy and Conservation Act (42 U.S.C. 6231-6247).

2. Title 42 U.S.C., Sections 2011, et seq. (Atomic Energy Act of 1954, as amended). Subchapter XVII, Enforcement, Section 2278a, sets forth the authority to issue regulations relating to the entry upon or carrying, transporting, or otherwise introducing or causing to be introduced any dangerous weapon, explosives, or other dangerous instrument or material likely to produce substantial injury or damage to persons or property, into or upon any facility, installation, or real property of DOE; establishes penalties for violating these regulations; and requires any such regulation to be posted.

3. Title 10 Code of Federal Regulations (CFR), Part 710, Subpart A, General, Criteria and Procedures for Determining Eligibility for Access to Classified Matter or Special Nuclear Material, establishes policies and procedures for DOE access authorizations.

4. Title 10 CFR, Part 860, Trespassing on Department of Energy Property, is issued for the protection of real property subject to the jurisdiction or administration of, or in the custody of, DOE.

5. Title 10 CFR, Part 1048, Trespassing on Strategic Petroleum Reserve Facilities and Other Property, is issued for the protection of the Strategic Petroleum Reserve facilities, related real property, and persons upon property that is subject to the jurisdiction or administration or in the custody of DOE under Part B, Title I of the Energy Policy and Conservation Act, as amended (42 U.S.C. 6231-6247).

6. Title 41 CFR, Chapter 101, Federal Property Management Regulations, sets forth introductory material concerning the Federal Property Management Regulations System and its content; types of property; related publications, including Federal specifications and standards; authority; applicability; numbering; deviation procedures; and Agency consultation, implementation, and supplementation.

7. DOE M 200.1-1, *Telecommunications Security Manual,* dated 3-1-97, provides for Communications Security program, including protection of crypto facilities.

8. DOE O 470.1, *Safeguards and Security Program,* dated 9-28-95, establishes general requirements; specifically paragraph 4f, which establishes the deviation process and responsibilities. It establishes specific requirements for planning and programs, including the following.

a. Chapter I, Safeguards and Security Program Planning, establishes a standard approach to safeguards and security (S&S) planning, including physical protection.

b. Chapter III, Performance Assurance Program, establishes a systematic process for demonstrating the adequacy and functional reliability of critical system elements.

c. Chapter V, Facility Clearances and Registration of Safeguards and Security Activities, establishes requirements for clearances and registration of facilities with S&S interests.

d. Chapter VIII, Control of Classified Visits Program, establishes requirements for controlling visitors to DOE and contractor, subcontractor, and access permitted facilities who need access to classified information.

9. DOE M 471.2-1C, *Classified Matter Protection and Control Manual,* dated 4-17-01. Provides detailed requirements for the protection and control of classified matter.

10. DOE O 472.1B, *Personnel Security Activities,* dated 3-24-97, establishes the requirements and responsibilities for implementing the Personnel Security Program.

11. DOE O 473.2, *Protective Force Program,* dated 6-30-00, prescribes requirements and responsibilities for the protective force program charged with the protection of S&S interests.

12. DOE M 473.2-2, *Protective Force Program Manual,* dated 6-30-00, prescribes requirements and detailed procedures for the protective force program.

13. DOE O 474.1A, *Control and Accountability of Nuclear Materials,* dated 11-20-00, prescribes requirements and responsibilities for control and accountability of nuclear materials.

14. DOE M 474.1-1A, *Manual for Control and Accountability of Nuclear Materials,* dated 11-22-00, prescribes requirements and procedures for nuclear material control and accountability.

15. DOE N 142.1, *Unclassified Foreign Visits and Assignments,* dated 7-14-99, establishes authorities, responsibilities, and policy, and prescribes administrative procedures for visits and assignments by foreign nationals to DOE facilities.

16. CG-SS-4, *Classification and UCNI Guide for Safeguards and Security Information,* Revision 1, dated August 2001, Office of Nuclear and National Security, provides classification determinations for National Security Information (NSI) concerning S&S and guidance for classifying documents and materials containing NSI, Formerly Restricted Data, and/or Restricted Data.

17. DOE *Technical Surveillance Countermeasures Procedural Manual (U),* dated October 1994. (This is an Office of Security document for limited distribution. Please call 301-903-3653 to request a copy).

18. "Design Basis Threat for Department of Energy Programs and Facilities (U)" of February 1999, issued by the Director of Security, identifies and characterizes the range of potential adversary threats to programs and facilities, which could adversely affect national security, the health and safety of employees or the public, the environment, or DOE S&S interests.

19. "Access Delay," Volume I, Technology Transfer Manual, SAND 2001-2168, Sandia National Laboratories, dated August 2001, defines the role of barriers in a physical protection program, provides penetration times for barriers, and defines methods for upgrading existing barriers.

20. "Alarm Communication and Display," Technology Transfer Manual, SAND99-2390, Sandia National Laboratories, dated 8-30-99, provides a description of the hardware and implementation techniques for an alarm communication and display system.

21. "Entry Control Systems," Technology Transfer Manual, SAND 2000-2142, Sandia National Laboratories, dated 9-30-00, compiles information regarding entry control systems and their application to physical protection programs.

22. "Explosive Protection," Technology Transfer Manual, SAND99-2486, Sandia National Laboratories, dated 8-30-99, discusses explosions the types of explosives, and the DOE detection and prevention of the introduction of explosives.

23. "Exterior Intrusion Detection," Technology Transfer Manual, SAND99-2391, Sandia National Laboratories, dated 8-30-99, discusses each class of detection systems, how to select the proper sensors, and how to combine them into an effective perimeter subsystem.

24. "Interior Intrusion Detection," Technology Transfer Manual, SAND99-2388, Sandia National Laboratories, dated 8-30-99, discusses the broad spectrum of sensors available, the physical principles by which each sensor operates, how the sensors interact with an intruder and the environment, and how the sensors interconnected with the system are monitored and assessed.

25. "Protecting Security Communications," Technology Transfer Manual, SAND99-2392, Sandia National Laboratories, dated 8-30-99, discusses the functions of a security communications network, its susceptibility to disruption, and the means by which security radio communications may be protected.

26. "Video Assessment," Technology Transfer Manual, SAND99-2389, Sandia National Laboratories, dated 8-30-99, discusses the design and uses of video alarm assessment systems, layouts, location of video system controls, and common construction and installation requirements and techniques.

27. ASTM E413-87(1999), "Standard Classification for Rating Sound Insulation," provides methods of calculating single-number acoustical ratings for laboratory and field measurements of sound transmission obtained in one-third octave bands. The method may be applied to laboratory or field measurements of the sound transmission loss caused by a partition in which case the single-number ratings are called Sound Transmission Class (STC) or Field Sound Transmission Class (FSTC), respectively.

28. ASTM F792-88 (1993), "Standard Practice for Design and Use of Ionizing Radiation Equipment for the Detection of Items Prohibited in Controlled Access Areas," covers the use of ionizing radiation imaging techniques for the detection of questionable items, such as weapons and devices intended to trigger explosives, in order to determine their presence in packages, or mail at screening points for controlling access to secure areas.

29. DCID 1/21, "Physical Security Standards for Sensitive Compartmented Information Facilities," dated 1-30-94, provides the construction requirements for the protection of classified information requiring extraordinary security safeguards.

30. DCID 6/2, "Technical Surveillance Countermeasures," dated 3-11-99, establishes the policy and procedures for the conduct and coordination of technical surveillance countermeasures.

31. DOE M 471.2-3A, *Special Access Program Policies, Responsibilities, and Procedures,* dated 7-11-02, provides guidance on special access procedures.

32. DOE M 452.4-1, *Protection of Use Control Vulnerabilities and Designs,* dated 7-1-99, provides guidance on the control and dissemination of Sigma 14 and 15.

33. DOE 5610.2, *Control of Weapon Data,* dated 8-1-80 with change 1, 9-2-86, provides the procedures for the definition and control of weapons Data.

34. DOE 1450.4, *Consensual Listening-In To or Recording Telephone/Radio Conversations,* dated 11-12-92.

35. Secretary of Energy Memorandum, dated 10-3-01; subject: Protection of Department of Energy and National Security Interests (U).

36. Department of Energy Badge Program, dated 12-1-00.

37. Underwriters Laboratories Inc. (UL) Standard 827, "Standard for Central-Station Alarm Services," dated 10-1-96.

38. UL Standard 681, "Standard for Installation and Classification of Burglar and Holdup Alarm Systems," dated 2-26-99.

39. UL Standard 752, "Standard for Bullet-Resisting Equipment," dated 3-10-00.

40. National Fire Protection Association 101, "Safety to Life from Fire in Buildings and Structures," dated 2000.

41. Federal Standard 809, "Neutralization and Repair of GSA-Approved Security Containers."

42. Federal Specification FF-L-2740A, "Locks, Combination."

43. American Society for Testing and Materials (ASTM) Standard F792-88, "Standard Practice for Design and Use of Ionizing Radiation Equipment for the Detection of Items Prohibited in Controlled Access Areas."

44. DOE *Sensitive Compartmented Information Facility Procedural Guide,* dated February 2, 2000.

45. CG-SS-4A, Annex to Classification and UNCI Guide for Safeguards and Security Information, Chapter 2, TSCM Requirements, dated June 2002.

46. "Safeguards and Security Glossary of Terms," available online at http://www.directives.doe.gov/libraries/othersources.html.

SECURITY BADGE SPECIFICATIONS

1. PURPOSE. The purpose is to set forth the information for implementing the Department of Energy (DOE) Security Badge Program and the badge specifications. While general requirements are cited in the *Physical Protection Program Manual* (DOE M 473.1-1) and this attachment to the Manual, specific badge design and implementation criteria are in Appendix 1 of this attachment. The details provided in Appendix 1, describing the configuration, encoding, and construction of the badges, necessitate marking the appendix "OFFICIAL USE ONLY" and releasing it by controlled distribution to the program offices and field elements.

2. SCOPE. Appendix 1 to this attachment has two parts.

   a. Part 1. Provides the information to develop a security badge that would be issued to DOE employees and DOE contractor employees.

   b. Part 2. Provides general design guidance for other types of badges designated as Local Site-Specific Only (LSSO) that may be issued within the Department. This would include badges issued to anyone other than DOE employees and DOE contractor employees.

3. APPLICATION. Badges that meet the requirements of Part 1 must be issued to DOE and DOE contractor employees. These badges must be accepted and used at other Departmental sites and facilities. The individual or organization being visited is responsible for verifying an individual's DOE access authorization level and determining need to know before granting access to special nuclear material or classified information.

   Badges that follow the requirements of Part 2 must not be used at any site or facility other than the site or facility where the badge was originally issued.

4. ISSUING AUTHORITY. The DOE Security Badge Program assigns to the issuing authority the responsibility for approving badges. The issuing authority must ensure badges meet the design requirements in this attachment and appendix. Any design parameters that are not met and which cause the DOE employee and DOE contractor badges to be unacceptable for access into other DOE sites must be resolved between the issuing authority and the site where access is being denied. The issuing authority is responsible for educating badge holders on the proper use and responsibilities associated with the DOE badges. This would include a program that informs individuals issued an LSSO badge, that the LSSO badge must only be used at the site where issued and will be confiscated if used in an attempt to inappropriately access other DOE facilities.

   Complexwide design issues, format parameters, and issues that pertain to Departmental badge policy are the responsibility of the Office of Security.

5. IMPLEMENTATION. The DOE Security Badge Program was implemented on November 18, 1998. Full implementation was to be completed in the following manner.

   a. Badges issued to DOE employees and DOE contractors (designed under provisions of Part 1) were to be issued by December 1, 2000. Any site or facility unable to meet the implementation schedule was to request up to a 1-year extension. Extension requests were to be directed to the program manager, Protection Program Operations, and to the respective program office or the National Nuclear Security Agency, as appropriate.

   b. Badges issued to foreign nationals (designed under provisions of Part 2) were to be issued by April 15, 1999.

6. CONTACT. Questions or suggestions concerning the program or specification and requests for copies of the appendix should be directed to the program manager, Protection Program Operations, at (301) 903-6209.

DEFINITIONS

1. Accepted Risk. Acknowledgment that a protection system may not achieve 100 percent protection against all occurrences, but further improvement in the system is not justified.

2. Barrier. A coordinated series of natural or fabricated impediment that direct, restrict, limit, delay, or deny entry into a designated area.

3. Cognizant DOE Official. The DOE line manager, or designee, with contract administration responsibility.

4. Concentric Security Areas. A series of physical spaces designated as security areas surrounding a designated safeguards and security interest. These security areas, property protection, limited, exclusion, protected, vital, and material access areas, provide for the imposition of graded physical protection measures which entail controlling access to and from the designated areas and security interests. Security areas are delineated by separate and distinct barriers and/or controls.

5. Credible Roll-up. A risk based evaluation of characteristics of the nuclear material and the security measures used to protect the material, based upon a performance standard. The determination of credibility of roll-up is unique for each facility. For example, risk evaluation includes but is not limited to the following.

   a. Material Characteristics—quantity of material, chemical form, isotopic composition or purity, ease of separability, possibility of concealment, portability, radioactivity, self-protecting features.

   b. Security Measures—containment strategy (e.g., types of drums or cans); accessibility (e.g., adversary task times); engineering controls (e.g., real-time inventory); administrative controls (e.g., access logs, accounting systems, tamper indicating devices); and protection strategies used by the facility. (See also ROLL-UP and RISK ANALYSIS.)

6. Design Basis Threat. Threats that are postulated for the purpose of establishing requirements for safeguards and security programs, systems, components, equipment, information or material.

7. Deviations. An approved condition that diverges from the norm that is categorized according to the degree of risk accepted as a variance, waiver, or exception.

8. False Alarm. An alarm, generated internal to the sensor equipment, for which the specific cause is unknown. Alarms caused by equipment malfunction.

9. Graded Protection. The levels of effort and magnitude of resources expended for the protection of safeguards and security interests which are commensurate with the security interests importance to loss, destruction, or misuse. The highest level of protection is afforded interests whose loss, theft or compromise, or unauthorized use would have serious impact upon national security and /or the health and safety of DOE and contractor employees, the public, the environment, or Department of Energy programs.

10. Hardened Structures. Exterior construction of walls, windows, doors, and floors and/or roof constructed of, or reinforced with, materials that have bullet-penetration resistance equivalent to the "high-powered rifle" rating cited in Underwriters Laboratories Inc. Standard 752, "Standard for Bullet-Resisting Equipment," dated 3-10-00.

11. Nuisance Alarm. Alarm produced by an intrusion detection sensor in response to a known stimulus (e.g., wind, lighting, thunder, accident) unrelated to an intrusion attempt.

12. Perimeter Intrusion Detection and Assessment System. A mutually supporting combination of barriers, clear zones, lighting, and electronic intrusion detection, assessment, and access control systems constituting the perimeter of the PA and designed to detect, impede, control, or deny access to the PA.

13. Piggybacking. Entering a security area with or behind a cleared authorized person who has vouched for the accompanying individual's authorization for access. (See also VOUCHING.)

14. Protection Strategies. Technical and tactical techniques to mitigate the design basis threats against special nuclear material, vital equipment, classified matter and government property. The strategies are for the protection of DOE assets from adversary actions that would impact the national security, the health and safety of employees, the public, or the environment.

15. Risk Analysis. An analysis of safeguards and/or security systems assets and vulnerabilities to establish an expected loss from certain events based on the estimated probabilities of those events

16. Risk Management. The integrated process of assessing the threat to, the vulnerabilities of, and the value of assets and applying cost-effective countermeasures. The process consists of five steps: (a) asset valuation and determination as to consequence of loss; (b) identification and characterization of the threats to specific assets; (c) identification and characterization of the vulnerability of specific assets; (d) identification of countermeasures, costs, and tradeoffs; and (e) risk assessment.

17. Roll-up (MC&A). The accumulation of smaller quantities of special nuclear material to obtain a higher category, based upon a compliance standard using the Graded Safeguards chart (DOE M 474.1-1A, *Manual for Control and Accountability of Nuclear Materials,* dated 11-22-00, Table I-4). The term "roll-up" simply refers to the total amount (isotopic

basis) of SNM that could be pulled together from various locations at a facility. If enough material exists when gathered together or surreptitiously diverted, then it would be evaluated at a higher category level. (See also CREDIBLE ROLL-UP)

18. Safeguards and Security Interest. Any DOE asset, resource or property which requires protection from malevolent acts. It may include but is not limited to classified matter, special nuclear material and other materials, secure communications centers, sensitive compartmented information facilities, automated data processing centers, facilities storing and transmitting classified information, vital equipment, or other DOE property.

19. Unknown Alarms. Alarms for which the cause is unidentified. These alarms may be caused by a real event but cannot be assessed because of poor lighting or degraded video. Reasonable efforts should be made to identify the cause of all alarms so that the number of unknown alarms is low. These alarms must be considered an intrusion until proven otherwise.

20. Validation. The confirmation by testing that an implemented, operational system or critical system element meets established requirements.

21. Verification. A process whereby information is evaluated relative to acceptance standards. In the context of site safeguards and plans, verification is considered to be a function of Headquarters security elements.

22. Vouching. Visually verifying the access authorization of another person for the purpose of piggybacking into a security area. (See also PIGGYBACKING.)

23. Vulnerability Analysis. A systematic evaluation process in which qualitative and/or quantitative techniques are applied to arrive at an effectiveness level for a safeguards and security system to protect specific targets from specific adversaries and their acts.