MANUAL

DOE M 470.4-2

Approved: 8-26-05
Review: 8-26-07

PHYSICAL PROTECTION

U.S. DEPARTMENT OF ENERGY
Office of Security and Safety Performance Assurance

AVAILABLE ONLINE AT:
http://www.directives.doe.gov

INITIATED BY:
Office of Security and Safety Performance Assurance

PHYSICAL PROTECTION

1. PURPOSE. This Manual establishes requirements for the physical protection of safeguards and security (S&S) interests.

2. OBJECTIVE. To effect the policy in DOE P 470.1, *Integrated Safeguards and Security Management Policy (ISSM)*, by integrating physical protection into DOE operations as determined by line management, and according to sound risk management practices. [DOE P 470.1, *Integrated Safeguards and Security Management Policy (ISSM),* is the Department's philosophical approach to the management of the S&S Program. A principal objective of the ISSM Program is to integrate S&S into management and work practices at all levels, based on program line management's risk management-based decisions, so that missions may be accomplished without security events, such as interruption, disruption or compromise. This approach includes individual responsibility and implementation of the security requirements found in this Manual.]

3. PROGRAM INTEGRATION. Physical protection must be integrated with other programs such as S&S program planning and management, protective force, information security, personnel security, and nuclear material control and accountability. The activities and requirements in the weapons surety, foreign visits and assignments, safety, emergency management, cyber security, intelligence, and counterintelligence programs should also be considered in the implementation of this Manual.

4. CANCELLATIONS. The directives listed below are canceled. Cancellation of a directive does not by itself modify or otherwise affect any contractual obligation to comply with the directive. Canceled directives that are incorporated by reference in a contract remain in effect until the contract is modified to delete the reference to the requirements in the canceled directives. The publication of this Manual incorporates all previous memoranda and letters that were issued by the Office of Security or its predecessor organizations that established policy.

   a. DOE M 473.1-1, *Physical Protection Program Manual*, dated 12-23-02.

   b. DOE M 471.2-1B, *Classified Matter Protection and Control*, dated 1-6-99.

5. APPLICABILITY.

   a. Departmental Elements. Except for the exclusion in paragraph 5.c., this Manual applies to all Departmental elements listed on Attachment 1. This Manual automatically applies to Departmental elements created after it is issued.

      The Administrator of the National Nuclear Security Administration (NNSA) will assure that NNSA employees and contractors comply with their respective responsibilities under this Manual.

b. Contractors.

(1) The Contractor Requirements Document (CRD), Attachment 2, sets forth requirements of this Manual that will apply to site/facility management contracts that include the CRD.

(2) The CRD must be included in the site/facility management contracts that involve classified information or matter, or nuclear materials, and contain DOE Acquisition Regulation (DEAR) clause 952.204-2, titled *Security Requirements*.

(a) Departmental elements must notify contracting officers of affected site/facility management contracts to incorporate this directive into those contracts.

(b) Once notified, contracting officers are responsible for incorporating this directive into the affected contracts via the *Laws, Regulations, and DOE Directives* clause of the contracts.

(3) A violation of the provisions of the CRD relating to the safeguarding or security of Restricted Data or other classified information may result in a civil penalty pursuant to subsection a. of section 234B, of the Atomic Energy Act of 1954 (42 U.S.C. 288b.). The procedures for the assessment of civil penalties are set forth in Title 10, Code of Federal Regulations (CFR), Part 824, *Procedural Rules for the Assessment of Civil Penalties for Classified Information Security Violations,* (10 CFR Part 824).

(4) As stated in DEAR clause 970.5204-2, titled *Laws, Regulations, and DOE Directives,* regardless of the performer of the work, site/facility contractors with the CRD incorporated into their contracts are responsible for compliance with the CRD. Affected site/facility management contractors are responsible for flowing down the requirements of the CRD to subcontracts at any tier to the extent necessary to ensure compliance with the requirements. In doing so, contractors must not unnecessarily or imprudently flow down requirements to subcontracts. That is, contractors must both ensure that they and their subcontractors comply with the requirements of this CRD and incur only costs that would be incurred by a prudent person in the conduct of competitive business.

(5) 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 as follows.

(a) Heads of Field Elements and Headquarters Departmental Elements. Review procurement requests for new non-site/facility management contracts that involve classified information or

matter, or nuclear materials and contain DEAR clause 952.204-2, titled *Security Requirements*. If appropriate, ensure that the requirements of the CRD of this Manual are included in the contract.

(b) Contracting Officers. Assist originators of procurement requests who want to incorporate the requirements of the CRD of this Manual in new non-site/facility management contracts, as appropriate.

c. Exclusion.

In accordance with the responsibilities and authorities assigned by Executive Order 12344, and to ensure consistency throughout the joint Navy and DOE organization of the Naval Nuclear Propulsion Program, the Deputy Administrator for Naval Reactors will implement and oversee all requirements and practices pertaining to this Manual for activities under the Deputy Administrator's cognizance.

d. Exemption.

(1) Requirements is this Manual that overlap or duplicate requirements of the Nuclear Regulatory Commission (NRC) related to radiation protection, nuclear safety (including quality assurance), and safeguards and security of nuclear material, do not apply to the design, construction, operation, and decommissioning of Office of Civilian Radioactive Waste Management (RW) facilities.

(2) This exemption does not apply to requirements for which the NRC defers to DOE or does not exercise regulatory jurisdiction.

6. DEVIATIONS. Deviations from the requirements in this Manual must be processed in accordance with DOE M 470.4-1, *Safeguards and Security Program Planning and Management*.

7. DEFINITIONS. Terms commonly used in the program are defined in the S&S Glossary located in DOE M 470.4-7, *Safeguards and Security Program References*. In addition to those in the Glossary, the following definitions are provided for use in this Manual.

a. DOE line management refers to DOE and NNSA Federal employees who have been granted the authority to commit resources or direct the allocation of personnel or approve implementation plans and procedures in the accomplishment of specific work activities.

b. Line management refers to DOE and NNSA Federal and contractor employees who have been granted the authority to commit resources or direct the allocation

of personnel or approve implementation plans and procedures in the accomplishment of specific work activities.

c. DOE cognizant security authority refers to DOE and NNSA Federal employees who have been granted the authority to commit security resources or direct the allocation of security personnel or approve security implementation plans and procedures in the accomplishment of specific work activities.

d. Cognizant security authority refers to DOE and NNSA Federal and contractor employees who have been granted the authority to commit security resources or direct the allocation of security personnel or approve security implementation plans and procedures in the accomplishment of specific work activities.

e. For the purposes of this Manual, the Office of Security refers to the DOE Office of Security at 301-903-6209.

8. 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 cognizant security authority and submitted to the relevant program officers; the Under Secretary for Energy, Science and Environment or the Under Secretary for Nuclear Security/Administrator, NNSA; and the Office of Security. The documentation must include timelines and resources needed to fully implement this Manual. The documentation must also include a description of the vulnerabilities and impacts created by the delayed implementation of the requirements.

9. CONTACT. Questions concerning this Manual should be directed to the Office of Security at 301-903-6209.

BY ORDER OF THE SECRETARY OF ENERGY:

CLAY SELL
Deputy Secretary

CONTENTS

SECTION A—PHYSICAL PROTECTION

CONTENTS (continued)

CONTENTS (continued)

CONTENTS (continued)

CONTENTS (continued)

SECTION B—SAFEGUARDS AND SECURITY ALARM MANAGEMENT AND CONTROL SYSTEMS (SAMACS)

SECTION A—PHYSICAL PROTECTION
CHAPTER I. PROTECTION PLANNING

1. PLANNING. The implementation of graded physical protection programs required by this Manual must be documented. Site physical protection programs must be systematically planned, executed, evaluated, and documented as described by a site safeguards and security plan (SSSP) or site security plan (SSP). Physical protection programs must be based on DOE O 470.3, *Design Basis Threat (DBT) Policy* (see DOE M 470.4-1, *Safeguards and Security Program Planning and Management*) and used in conjunction with local threat guidance.

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

   b. Departmental assets must be protected from malevolent acts such as theft, diversion, and sabotage and events such as natural disasters and civil disorder by considering site and regional threats, protection planning strategies, and protection measures. Special nuclear material (SNM) must be protected at the higher level when credible roll-up to Category I quantities can occur within a single security area unless the facility has conducted a vulnerability assessment that determined the failure or defeat of protection measures would not decrease system effectiveness. The Department has the authority to impose requirements deemed necessary to protect the safety of employees and the public and to minimize threats to life, SNM, radiological/chemical/biological materials, classified information or matter, Government property, the public, and the environment.

   c. Sites upgrading security measures must consider the benefits provided by security technology through the conduct of life cycle cost benefit analysis, comparing the effectiveness of security technology to traditional manpower-based methodologies.

2. PROTECTION STRATEGIES. Protection strategies, as described in DOE M 470.4-1, *Safeguards and Security Program Planning and Management*, must be selected, developed, and implemented to protect S&S interests.

3. GRADED PROTECTION. Protection must be applied in a graded manner that is commensurate with S&S interests (see DOE M 470.4-1, *Safeguards and Security Program Planning and Management*).

4. PERFORMANCE ASSURANCE. Physical protection systems, including components, must be tested to ensure overall system effectiveness. The effectiveness of physical protection systems and programs must be determined through performance testing, at least annually (at least every 12 months), as required by the performance assurance program. A program of scheduled testing and maintenance must be implemented to

ensure an effective, fully functional security system (see DOE M 470.4-1, *Safeguards and Security Program Planning and Management*).

5. PHYSICAL PROTECTION SURVEILLANCE EQUIPMENT.

   a. Physical protection surveillance equipment must be used for the purposes described in an SSSP or SSP. Procedures must be developed to prohibit misuse of physical protection surveillance equipment (e.g., video assessment and audio communication/recording equipment). NOTE: Physical protection surveillance equipment, when used in accordance with this requirement, is not considered technical surveillance equipment.

   b. Signs must be posted to serve notice that physical protection surveillance equipment is in operation.

6. SAFETY AND HEALTH. S&S programs must meet mission objectives and the DOE safety and health objectives to protect workers (see DOE M 411.1-1C, *Safety Management Functions, Responsibilities, and Authorities*).

7. TRAINING. Personnel implementing the physical protection program may meet physical security protection competencies within the Professional Development Program of the DOE National Training Center (NTC).

CHAPTER II. PROTECTION OF NUCLEAR WEAPONS, COMPONENTS, SPECIAL NUCLEAR MATERIAL, AND CLASSIFIED INFORMATION AND MATTER

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, diversion, and radiological sabotage and to respond to adverse conditions such as emergencies caused by acts of nature. SNM must be protected at the higher level when credible roll-up (e.g., Category II quantities to a Category I quantity of SNM) can occur unless the facility has conducted a vulnerability assessment that determined that the failure or defeat of protection measures would not decrease system effectiveness.

   a. A facility must not possess, receive, process, transport, or store nuclear weapons or SNM until that facility has been cleared commensurate with DOE M 470.4-1, *Safeguards and Security Program Planning and Management*.

   b. An integrated 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 separation, accessibility, concealment, portability; radioactivity; and self-protecting features.

   d. The protection of nuclear material production, reactors, and fuel must be commensurate with the category of SNM.

   e. SNM, parts, or explosives that are classified must receive the physical protection required by the highest level of classification or category of SNM, whichever is the more stringent.

   f. Specific physical protection measures and protective force (PF) response capabilities must be described in a Site Safeguards and Security Plan (SSSP) or Site Security Plan (SSP).

   g. The protection afforded SNM must be graded, according to the nuclear material safeguards category and attractiveness level, and reflect the specific nature of the nuclear weapons or SNM at each site.

2. ACCESS. Access controls must be in place to ensure that only appropriately cleared and authorized personnel are permitted unescorted access to SNM and nuclear weapons. Access authorizations must be granted commensurate with DOE M 470.4-5, *Personnel Security*.

3. INTRUSION DETECTION SYSTEM. Nuclear weapons and Category I and II quantities of SNM must be protected by an integrated physical protection system using PF, barriers, and intrusion detection systems (IDS) that annunciate at a central alarm station (CAS).

4. DELAY MECHANISMS (BARRIERS). Mechanisms must be used to deter and delay access, removal, or unauthorized use of Category I and II quantities of SNM and nuclear weapons. 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 response capability must be used to deny, neutralize, contain, and/or perform recapture/recovery and pursuit missions within the required timelines (see DOE M 470.4-3, *Protective Force*).

6. STORAGE CONTROLS. Each facility must have controls for nuclear weapons and SNM consistent with the graded safeguards approach required by paragraphs 7 through 10 below. 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 and document SNM movement into, or out of, a storage location;

   e. include procedures for investigating and reporting abnormal conditions;

   f. provide a record system to document ingress and egress; and

   g. define procedures for conducting daily administrative checks.

7. CATEGORY I QUANTITIES OF SPECIAL NUCLEAR MATERIAL. The following requirements apply:

   a. In Use or Processing. Category I quantities of SNM must be located within a material access area (MAA) inside a protected area (PA). Any MAA containing unattended Category I quantities of SNM must be equipped with an IDS or other means of detection approved by the cognizant DOE line management.

   b. Storage. Category I quantities of SNM must be stored within an MAA.

      (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 (VTR) storage (e.g., collocated with a PF response station and/or activated barriers).

(3) Category I, attractiveness level C, SNM must be stored in a VTR.

c. Transportation. The following requirements apply:

(1) Domestic off-site SNM shipments must be made by the Office of Secure Transportation (OST).

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

(3) Protection measures for movements of the SNM, between PAs at the same site or between PAs and staging areas on the same site, must be under constant surveillance by armed PF escorts.

8. CATEGORY II QUANTITIES OF SPECIAL NUCLEAR MATERIAL. The following requirements apply:

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

b. Storage. Category II quantities of SNM must be stored in a vault or VTR located within a PA.

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

9. CATEGORY III QUANTITIES OF SPECIAL NUCLEAR MATERIAL. The following requirements apply:

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

b. Storage. Category III quantities of SNM must be stored within a locked security container or room, either of which must be located within at least an LA. The container or room must be under the protection of an IDS or PF patrol physical check at least every 8 hours.

c. Transportation. Category III quantities of SNM may be transported by the following methods unless otherwise prohibited by statute (see DOE O 460.2A, *Departmental Materials Transportation and Packaging Management*).

(1) Domestic off-site shipments of classified configurations of Category III quantities of SNM must be made by the OST.

(2) Off-site shipments of unclassified configurations of Category III quantities of SNM are not required to be made by OST. If OST is not used, such shipments may be transported by the following authorized methods:

(a) Truck or train shipment. The following requirements must be met:

1 Government-owned or exclusive-use truck, commercial carrier, or rail may be used;

2 transport vehicles must be inspected before loading and shipment. Cargo compartments must be locked and sealed after the inspection and remain sealed while enroute;

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 (LLEA) response if needed; and

4 no intermediate stops are permitted except for emergencies, driver relief, meals, refueling, or transfer of security interests.

(b) Air Shipment. Shipments must be under the direct observation of the authorized escorts during all land movements and loading and unloading operations.

(3) Movement between security areas at the same site must comply with the locally developed shipment security plan.

10. CATEGORY IV QUANTITIES OF SPECIAL NUCLEAR MATERIAL. The following requirements apply:

a. In Use or Processing. The SNM must be used or processed within at least a property protection area (PPA) and in accordance with local security procedures approved by DOE line management.

b. Storage. The SNM must be stored in a locked area within at least a PPA, and procedures must be documented in an approved SSP or SSSP.

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

(1) Domestic off-site shipments of classified configurations of Category IV quantities of SNM may be made by the Office of Secure Transportation or by other means when approved by DOE line management.

(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 made by a mode of transportation that can be traced and, within 24 hours of request, the last known location of the shipment can be determined. This process must be implemented if a shipment fails to arrive at its 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. Upon initial notification, the shipper must report commensurate with DOE M 470.4-1, *Safeguards and Security Program Planning and Management.*

11. PROTECTION OF CLASSIFIED INFORMATION OR MATTER. The following are general requirements for the protection of classified information or matter. Detailed requirements for the protection of classified information or matter can be found in DOE M 470.4-4, *Information Security*. In general:

a. Classified information or matter is any combination of documents and material containing classified information. This includes classified parts and explosives whose shapes are considered classified. The secure storage requirements are described in Chapter XI.

b. Classified matter must be processed, handled, or stored in security areas that provide protection measures equal to or greater than those present in an LA in accordance with Chapter IV.

c. 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.

d. 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.

e. Buildings and rooms containing classified matter must have the security measures necessary to deter unauthorized persons from gaining access to classified matter. This includes 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 (TSCM) program requirements (see DOE M 470.4-4, *Information Security*).

12. VITAL EQUIPMENT. SSPs and SSSPs must define applicable threats to and protection measures for vital equipment.

CHAPTER III. 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 special nuclear material (SNM) must be in accordance with Chapter II and this Chapter. The physical protection against radiological, chemical, or biological sabotage must adhere to DOE O 470.3, *Design Basis Threat (DBT) Policy*.

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

   b. Radiological, chemical, or biological sabotage targets must be provided protection as determined by vulnerability analyses

2. ANALYSIS. Facilities with a radiological, chemical, or biological sabotage threat must document the sabotage analysis process and the program for protection in a Site Safeguards and Security Plan (SSSP) or Site Security Plan (SSP) commensurate with DOE M 470.4-1, *Safeguards and Security Program Planning and Management*.

   a. Emergency and Safety. Safety analysis reports, emergency planning hazards assessments (see DOE O 151.1B, *Comprehensive Emergency Management System,* dated 10-29-03), vulnerability assessment reports, accident scenarios, emergency event classifications, protective actions, consequence calculations, and any other pertinent information must be considered in the radiological, chemical, or 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, or biological sabotage.

3. RADIOLOGICAL, CHEMICAL, OR BIOLOGICAL SABOTAGE. Physical protection strategies must be developed, documented, and implemented consistent with the DBT to protect radiological, chemical, or biological sabotage targets.

   a. Radiological. Targets must be protected in a graded manner to protect S&S interests and to mitigate consequences of a radiological sabotage event.

   b. Chemical. Targets must be protected to protect S&S interests and to mitigate consequences of a chemical sabotage event.

   c. Biological. Targets must be protected to protect S&S interests and mitigate consequences of a biological sabotage event.

d. Mitigation. The implementation of the following prevention and mitigation measures must be based on the results of the radiological, chemical or 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 IV. SECURITY AREAS

1. GENERAL REQUIREMENTS. Security areas include Property Protection Areas (PPA), Limited Areas (LAs), Exclusion Areas (EAs), Protected Areas (PAs), Vital Areas, Material Access Areas (MAAs), and specially designated security areas [e.g., Sensitive Compartmented Information Facilities (SCIFs) and Special Access Program Facilities (SAPFs)].

   a. Prohibited Articles. Authorization of prohibited articles to be used for official Government business must be documented in a Site Safeguards and Security Plan (SSSP) or Site Security Plan (SSP). The articles listed below are not permitted in any security area without authorization, unless identified in approved local procedures:

      (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); and

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

   b. Controlled Articles. Portable electronic devices, both Government- and personally-owned, capable of recording information or transmitting data (e.g., radio frequency, infrared, and/or data link electronic equipment) are not permitted in LAs, EAs, PAs, Vital Areas, MAAs, SCIFS, or SAPFs without authorization. DOE line management must use the following criteria in authorizing the use of this equipment:

      (1) the equipment, including those electronic devices having multiple built-in electronic recording and transmitting capabilities, is essential to the mission;

      (2) the equipment is Government-owned or -leased; and

      (3) documented risk analysis has been performed, identifying vulnerabilities inherent to the characteristics and operation of the device along with defined countermeasures.

      NOTE: 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. Security interests must be protected using a concentric security areas approach as described below.

a. Concentric Security Areas. Layers of security requirements, beginning with the least restrictive and moving inward to the most restrictive, must be implemented for protecting safeguards and security (S&S) interests. Security areas designated as LAs, EAs, PAs, Vital Areas, or MAAs must be established to protect S&S interests. These areas must be defined by permanent barriers, and access to these security areas must be controlled based on need-to-know and need-for-access.

b. Access. Access 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 trained in local escort procedures.

(2) The cognizant security authority must establish escort-to-visitor ratios in a graded manner for each security area.

c. Entry/Exit Inspections. Entry/exit inspections are required at PAs and MAAs, as described in paragraphs 6. and 8. of this Chapter, and at other security areas as required by DOE line management and documented in the SSSP or SSP. Entry inspections of personnel, hand-carried items, packages, and/or vehicles must ensure prohibited articles are detected and are not introduced without authorization. Exit inspections must ensure S&S interests are not removed without authorization (see Chapter VIII).

d. Emergency Personnel and Vehicles. Emergency personnel and vehicles may be authorized for immediate entry in response to an emergency. The conditions and procedures for immediate entry must be documented in the SSSP or SSP. Emergency personnel and vehicles must be inspected when exiting post-emergency or when leaving the site. If the emergency condition prevents an exit inspection before departing the site, an escort must be provided to ensure that both personnel and emergency vehicles are inspected as soon as the emergency is terminated.

e. Signs. Signs prohibiting trespassing must be posted around the perimeter and at each entrance to a security area except when one security area is 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 provides details on posting requirements [see 42 United States Code (U.S.C.) Section 2278a and Section 229].

f. Parking Areas.

(1) If parking areas are near security areas and could interfere with intrusion detection sensor fields, clear zones, or Protective Force (PF) operations, these parking concerns must be addressed in the SSSP or SSP.

(2) The threat posed by a vehicle bomb must be considered in the placement of vehicle parking areas.

g. Visitor Logs. Visitor logs must be used for EAs, PAs, and MAAs.

(1) Site-specific requirements and procedures for visitor logs must be developed and approved by DOE line management. The procedures must provide for recording the following visitor information: printed name and signature, agency or organization represented, citizenship, person to be visited, purpose of the visit, time of entry and exit.

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

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

(4) Visitor logs must plainly reflect the penalty of false personation and representation.

(a) Laws regarding the penalty for false personation are stated in 18 U.S.C. Part 1, Section 911.

(b) Laws regarding fraud and false statements are stated in 18 U.S.C., Part 1, Section 1001.

h. Permanent Physical Barriers. Permanent physical barriers must identify the boundary of a security area and achieve the following objectives as well as meet the requirements described in Chapter IX.

(1) Barriers must be capable of controlling, impeding, or denying access to a security area. Barriers are used to:

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

(b) delay and/or deter the introduction of prohibited and controlled articles or the removal of S&S interests; and

(c) delay and/or prevent penetration of a security area by vehicles.

(2) Penetrations of Security Area Barriers.

(a) Overhead utilities must not pass between security areas without physical protection features to prevent unauthorized access into the security area.

(b) Elevators that penetrate a security area barrier must be provided with an access control system that 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 the barriers they penetrate. This applies when the unattended opening within the utility corridor meets the requirements of Chapter IX, paragraph 8.b.(1).

(d) Objects that intruders could use to scale or bridge barriers and enter security areas must be removed or secured to prevent their unauthorized use.

(e) If a barrier configuration is altered, barriers must be erected (e.g., during construction or temporary activities), and a vulnerability assessment must be conducted to validate equivalent protection measures.

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, access control systems, protective personnel or persons assigned administrative or other authorized security duties, Intrusion Detection System (IDS), and locks and keys. The designation of and description of PPA protective measures must be approved by DOE line management (e.g., SSP or SSSP). The requirements for PPAs must be configured to protect Government-owned property and equipment against damage, destruction, or theft and must provide a means to control public access.

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).

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. LAs are security areas designated for the protection of classified matter and Category III quantities of special nuclear material (SNM).

   a. General Requirements. LAs are defined by physical barriers encompassing the designated space and access controls to ensure that only authorized personnel are allowed to enter and exit the area. A means must be provided to detect unauthorized entry into the LA. LA access requirements must be administered as follows.

      (1) Individuals without appropriate access authorization must be escorted by an authorized individual who must ensure measures are taken to prevent compromise of classified matter or access to SNM.

      (2) Access to S&S interests, not in approved storage within an LA, must be controlled by the custodian or authorized user.

   b. Personnel and Vehicle Access Control.

      (1) The identity and access authorization of each person seeking entry must be validated by PF or other appropriately authorized personnel, automated systems, or other means documented in the SSSP or SSP.

      (2) Validations must occur at entry control points of LAs.

      (3) Private vehicles are prohibited from LAs unless specifically authorized in writing. Approval authority for non-Government vehicle access must be documented in the SSSP or SSP.

      (4) Government-owned or -leased vehicles may be admitted only when on 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 SSSP or SSP must identify procedures for inspection of and access by service and delivery vehicles.

      (5) When a remote automated access control system is used for vehicle access control, it must verify that the operator or the escort has 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 SSP, may be used to validate the badge and access authorization at automated entry control points.

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

   a. General Requirements. The boundaries of EAs must be encompassed by physical barriers. EAs require access controls that ensure only authorized personnel are

allowed to enter and exit the area. Examples of means to detect unauthorized entry into the EA include; PF patrols, closed circuit television (CCTV) systems, IDS, or a combination of measures. Unauthorized entry into the EA must be detected. EA requirements are as follows.

(1) Individuals permitted unescorted access must have "L" or "Q" access authorizations and a need-to-know consistent with the classified matter to which they have access by virtue of their presence in the area.

(2) Individuals without "L" or "Q" access authorization and need-to-know must be escorted by a knowledgeable individual who must ensure measures are taken to prevent compromise of classified matter.

(3) EAs protecting SNM must provide protection as specified in Chapter II.

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 LAs apply to EAs (see 4.b., above).

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

a. General Requirements. PAs must be encompassed by physical barriers that identify the boundaries, surrounded by a perimeter intrusion detection assessment system (PIDAS), and equipped with access controls that ensure only authorized personnel are allowed to enter and exit.

b. Barriers.

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

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

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

(4) The barrier design must consider proximity to buildings or overhanging structures.

(5) The barrier design must consider the attempted removal of S&S interests by an insider.

c. Intrusion Detection and Assessment. A PA must be encompassed by a PIDAS. The PIDAS must be monitored in a continuously manned CAS and a secondary alarm station (SAS). Specific requirements for PIDAS are listed in Chapter VII.

d. Entry Control Points. PA entry control point systems must allow the authorized entry of personnel while detecting prohibited and controlled articles. Entry control point design must include separate material package inspection stations for inspecting personnel, packages, and hand-carried items. The following design criteria apply:

(1) Entry/exit point inspection monitors must be collocated with PF posts to facilitate the initiation of a response to an alarm.

(2) PF posts must be designed with an unobstructed view to facilitate observation of any attempt to bypass systems.

(3) Hardened PF posts must meet the requirements of Section A, Chapter VI, paragraph 2.a.

e. PA Access. The following requirements apply:

(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 personnel, vehicles, packages, and hand-carried items must be performed to deter and detect the unauthorized removal of SNM and other Government property. Specific inspection procedures with limitations and thresholds for SNM detectors and metal detectors must be established and documented in the SSSP or SSP. Exit inspection procedures must be written to ensure:

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

(b) the detection of shielded SNM (e.g., by using a combination of SNM detectors and metal detectors).

(c) that entry control points without the means to detect SNM are not used to exit, except in emergencies.

(d) the conduct of random exit inspections at a PA boundary, when a PA encompasses an MAA and the Category II or greater quantities of SNM are contained completely within the MAA. The frequency must be determined by DOE line management.

(e) that equivalent protection measures are implemented when emergency exits are used (e.g., searches are conducted at an assembly area).

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

f. Personnel Access Control. The following requirements apply:

(1) The identity and access authorization of each person seeking entry must be validated by armed PF personnel; or

(2) If PA access is controlled by an unattended automated access control system, the system must verify the following:

(a) a valid DOE security badge (the badge serial number read by the system must match the serial number assigned to the badge holder);

(b) valid access authorization; and

(c) valid personal identification number (PIN).

(3) Protective personnel or other means documented in the SSSP/SSP may be used to validate the badge and access authorization at automated entry control points. Additional details can be found in Chapter VIII.

g. Vehicle Access Controls. The following requirements apply:

(1) Private vehicles are prohibited.

(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 separate security areas that contain vital equipment within PAs.

a. General Requirements. In addition to the protection strategies required for PAs, the following requirements must be applied:

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

(2) the perimeter must be monitored to deter and detect unauthorized entry attempts.

(3) vital equipment must be protected with an IDS.

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

(5) PF response time to an intrusion alarm must be less than the delay time that can be demonstrated from the time an alarm is activated at the PA boundary to task completion.

(6) all requirements for personnel and vehicle access control that apply to PAs (see 6.f. and g., above) apply to Vital Areas.

8. MATERIAL ACCESS AREAS. MAAs are security areas used to protect Category I quantities of SNM or credible roll-up quantities of SNM to a Category I quantity.

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 a PA, but must be separate and distinct (i.e., no shared boundaries); however, multiple MAAs may exist within a single PA. An MAA cannot cross a PA boundary.

(2) Barriers must delay or deter the unauthorized movement of SNM, while allowing access by authorized personnel and 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 the time an alarm is activated at the PA boundary to task completion.

(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 or diversion of S&S interests.

(5) Exits designed for emergency evacuation must be alarmed with an IDS or controlled at all times.

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

(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 personnel, vehicles, packages, and hand-carried items must be performed to deter and detect the unauthorized removal of SNM and other Government property. Specific inspection procedures with limitations and thresholds for SNM detectors and metal detectors must be established and documented in the SSSP or SSP.

(a) A separate physical or electronic inspection of each vehicle, person, package, and container must be conducted at all MAA exit points.

(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 MAA.

(c) Exit inspections must be capable of detecting shielded SNM (e.g., by using a combination of SNM detectors 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 and access authorization of each person seeking entry must be validated by armed PF personnel; or

(2) If MAA access is controlled by an unattended automated access control system, the system must verify:

(a) a valid DOE security badge (the badge serial number read by the system must match the serial number assigned to the badge holder);

(b) a valid access authorization; and

(c) a valid PIN.

(3) Protective personnel, or other means documented in an SSSP, may be used to validate the badge and access authorization at automated entry control points.

(4) Private vehicles are prohibited from entry.

(5) 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

9. SPECIAL DESIGNATED SECURITY AREAS. Other areas with access restrictions include CASs, SASs, SCIFs, Special Access Program (SAP) Facilities, LLEA 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, and DOE M 470.4-1, *Safeguards and Security Program Planning and Management*.

b. Alarm Stations. CAS and SAS requirements are described in Chapter V.

c. Sensitive Compartmented Information Facilities. DOE follows the requirements in Director of Central Intelligence Directive 6/9, DOE Order 5639.8A, *Security of Foreign Intelligence Information and Sensitive Compartmented Information Facilities*, dated 7-23-93, and DOE *Sensitive Compartmented Information Facility Procedural Guide* for the construction and accreditation of SCIFs.

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

e. Secure Communications Centers and Automated Information System Centers.

(1) All centers for handling classified information must be located in an LA.

(2) Separate access controls and barriers must be established to restrict entry 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 are required for all persons assigned to or having unescorted access to these centers. A list of persons who have authorized access must be maintained within the center, and a record must be maintained of all visitors entering the facility.

(4) The design of automated information systems centers and remote interrogation points that process classified information must consider the following.

(a) Control Zone is the space above, below, and around equipment and distribution systems that can be inspected and is under physical and technical control to prevent unauthorized access.

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

CHAPTER V. ALARM MANAGEMENT AND CONTROL SYSTEM

1. GENERAL REQUIREMENTS. This Chapter establishes requirements for integrated physical protection systems protecting safeguards and security (S&S) interests. All intrusion detection system (IDS) sensors 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 initiating responses to S&S incidents.

      (1) Alarm stations must be attended continually.

      (2) Private or local law enforcement agency (LLEA) alarm station personnel must be knowledgeable of the area being protected and the emergency notification procedures. Knowledge of the area does not encompass the operations contained therein or what is stored or processed. As an example, area knowledge would involve the building alarm configuration; room numbers within the structure; pedestrian and vehicle entry points, etc.

      (3) Tamper and supervisory alarms must be assessed by protective force (PF) personnel. Technical/maintenance support personnel must conduct follow-up assessments of tamper and supervisory alarms.

      (4) Acknowledgment of alarms must be a simple and non-complex process and easily performed.

      (5) When closed-circuit television (CCTV) systems are used, the alarm control system must be able 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.

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

      (7) When used as the primary means of alarm assessment and to determine response level, CCTV systems must annunciate when the video signal from the camera is lost or disrupted.

      (8) 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.

(9) Records must be kept of each alarm received in the alarm station and of any maintenance activities conducted on the alarm system or any of the related components.

b. Alarm Station Architectural Requirements. The alarm station must be of sound construction and meet local building codes.

2. HIGH-CONSEQUENCE FACILITIES. Facilities with Category I and II quantities of special nuclear material (SNM), or other high-consequence targets as identified by vulnerability assessments, must have a Central Alarm Station (CAS) and a Secondary Alarm Station (SAS).

a. CAS and SAS Requirements.

(1) Personnel must possess access authorizations (i.e., Q or L) commensurate with the most sensitive asset under the protection of the alarm station.

(2) Access control systems must ensure admission of authorized personnel only.

(3) Alarms must annunciate both audibly and visibly as well as simultaneously to the CAS and the SAS.

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

(5) The CAS and SAS must be physically separated.

(6) 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 be designed as a hardened post, located within an limited area (LA) and manned 24 hours a day.

(2) Exterior walls, windows, doors, and roof must be constructed of, or reinforced with, materials that have a bullet-penetration resistance equivalent to the Level 8 rating given in Underwriters Laboratories Inc., Standard 752, “Standard for Bullet-Resisting Equipment” (UL-752).

(3) Entryways must be fitted with doors equipped with locks that can be operated from within the alarm station.

c. Additional SAS Requirements. The SAS must be used as an alternative alarm annunciation point to the CAS and be manned 24 hours a day so that a response can be initiated if the CAS cannot perform its intended function. The SAS may be located in a PPA. The SAS need not be fully redundant to the CAS, but must be capable of providing full command and control in response to S&S incidents [see 2.a.(6), above].

3. CLOSED-CIRCUIT TELEVISION SYSTEM. CCTV assessment systems must be functional under day, night, overcast, and artificial lighting conditions. The system must provide 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 are as follows:

(1) the system must have the capability to automatically switch to the camera associated with the alarm event and to display that event for operator assessment;

(2) video recorders must be actuated by the intrusion alarm and record automatically;

(3) video recorder response time must be rapid enough to record the actual intrusion and able to capture sufficient information for alarm assessment;

(4) video assessment coverage must be complete (e.g., no gaps between zones or areas that cannot be assessed because of shadows or objects blocking the camera's field of view);

(5) CCTV used for primary assessment must be tamper protected and use fixed cameras with fixed focal length lenses that provide a clear image for assessment (pan-tilt-and-zoom cameras may be used for surveillance);

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

(7) the video system must accept manual override of automatic features. This capability permits the operation of a CCTV camera associated with another event.

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 VII.

5. FUTURE SYSTEMS. The requirements for Safeguards and Security Alarm Management and Control Systems (SAMACS) used in the protection of Category I and II quantities of SNM and installed and operational after January 1, 2008, are contained in Section B. Section B contains "Unclassified Controlled Nuclear Information" and will be issued separately from this Manual. A copy of the SAMACS document may be obtained by contacting the Program Manager, Protection Program Operations at 301-903-6209.

CHAPTER VI. PROTECTION OF SECURITY SYSTEM ELEMENTS

1. GENERAL REQUIREMENTS. Security-related equipment must be protected from unauthorized access in a graded manner consistent with the security interest under protection. Central Alarm Stations (CAS) and Secondary Alarm Stations (SAS) must be protected in accordance with Chapter VII. Commercial CAS must have current Underwriter's Laboratory (UL) Class AA installation and must maintain this UL certification. Sensitive Compartmented Information Facility (SCIF) Intrusion Detection Systems (IDS) must meet the requirements of the Director of Central Intelligence Directive and the *DOE Sensitive Compartmented Information Facility Procedural Guide*.

2. PROTECTIVE FORCE POSTS.

   a. Special Nuclear Material Access. Permanent Protective Force (PF) posts controlling access to Protected Areas (PA) and Material Access Areas (MAA) must be constructed to meet the requirements for a hardened post. Exterior walls, windows, roofs, and doors must be constructed of, or reinforced with, materials that have a bullet-penetration resistance equivalent to the Level 8, High Power Rifle rating given in UL-752, *Bullet Resisting Equipment*.

   b. Lighting. Lighting must provide 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 operation from inside the post.

   d. Protective Force Towers. PF towers that are intended to be used as fighting positions must be bullet-penetration resistant equivalent to the High Power Rifle rating given in UL-752, *Bullet Resisting Equipment*.

3. INTRUSION DETECTION SYSTEMS. The requirements for physically protecting IDS components are as follows:

   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/field processors), and transmission lines from field processors to annunciators and/or alarm stations.

   b. Enclosures and Junction Boxes. Electronic enclosures and junction boxes must be secured to preclude 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 IDS protecting safeguards and security (S&S) interests. For Property Protection Areas (PPA), line supervision may be provided consistent with a documented cost/benefit analysis as determined by each facility. Where data encryption is used, key changes must be made annually (at least every 12 months) and whenever compromise is suspected. The requirements for line supervision are listed below (see Table 1., Line Supervision Protection).

(1) Line Supervision Options. Different combinations of line supervision are allowed depending on link routing:

(a) alarm communication link remaining within the security area; and

(b) alarm communication link going through a lower security area.

(c) Line supervision is required for the two primary segments of alarm data transmission: from sensor to field processor and from field processor to field processor or the 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 field processors, between field processors and central alarm computers or alarm annunciator panels, and between computers.

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

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

a encryption using a proprietary encryption scheme that results in non-repetitive communications;

b pseudo-random polling scheme;

c non-encryption over fiber optic cable enclosed in conduit; or

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

3 For Class C, unencrypted data transmissions include:

a RS-232, RS-485, etc., data transmission standard;

b standard repetitive polling schemes; and

c exception reporting with repetitive polling for health checks.

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

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.

(3) Protecting Alarm Wiring. Physical protection of alarm wiring must be as listed below.

(a) Protection for communication links must meet the requirements for the National Electric Code for protection from damage per Underwriters Laboratories Inc., Standard 681 "Installation and Classification of Burglar and Holdup Alarm Systems" (UL-681).

(b) Protection for wiring between the sensor and the field processor using Class F line supervision must be protected from access. Acceptable methods for protecting alarm system wiring must use:

1 a totally concealed or embedded conduit system;

2 threaded conduit (i.e., rigid or intermediate metal conduit) for all connections of exposed conduit;

3 seal junction boxes, pull boxes and other openings by welding, epoxy sealed threads, locked cover plates, tamper-resistant screws, or tamper alarm switches; or

4 alarm coverage of all wiring.

(4) Tamper Switch Wiring. Tamper switch wiring must be as listed below.

(a) For communication links, field processors and associated equipment must be provided with tamper detection switches on enclosure covers wired to a 24-hour circuit. The wiring must be protected from unauthorized access, per UL-681.

(b) For wiring between a sensor and field processor, tamper switches must be wired into a 24-hour circuit. More than one switch may be

wired to a single circuit if the switches are located in the same general area.

(c) The switches may be wired as part of the line supervision circuit, per UL-681. However, tamper switches may be wired 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 using a separate circuit.

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

(3) PF personnel must be put on alert, and system maintenance personnel must be notified, when line supervision alarms indicate a loss of a 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 PF response personnel (see Chapter XIII).

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

(b) Tamper and line supervision alarms must be tested to verify effectiveness. Alarm system components being protected by the tamper alarm [e.g., balanced magnetic switch [BMS], microwave, passive infrared] must be tested through physical actuation (see Table 1., Line Supervision Protection).

Table 1. Line Supervision Protection

Communication Lines between a Field Processor and Field Processor or a Central Processor				
	Cat I or II SNM, Vital Equipment, or Top Secret Classified Matter Class of Supervision	Cat III or IV SNM, Classified Matter Secret and below Class of Supervision	Maximum Internal System communications supervision interval (ALL)	Required Manual Testing (ALL)
Routed within the alarm area	C	C	15 Minutes	Annually*
Routed through a lower security area	B	C	10 minutes	Annually*
Routed through an unsecured area	A	B	5 minutes	Annually*
Wiring from the Sensor to the Data Gathering Panel				
All field wiring	F	F	Continuously	Annually*

* at least every 12 months

CHAPTER VII. INTRUSION DETECTION AND ASSESSMENT SYSTEMS

1. GENERAL REQUIREMENTS. Intrusion detection and assessment systems and/or visual observations by Protective Force (PF) personnel must be used to protect special nuclear material (SNM), classified matter, and Government property to ensure breaches of security barriers or boundaries are detected and alarms annunciate. 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) Intrusion detection and assessment must be immediate.

      (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.

      (3) Perimeter Intrusion Detection Assessment Systems (PIDAS) must use multilayered, complementary intrusion detection sensors.

   b. Assessment of Intrusion Detection System Alarms. An effective method must be established for assessing all Intrusion Detection System (IDS) alarms (e.g., line supervision, intrusion, false, nuisance, system failure, tamper, and radio frequency alarms when radio frequency is used) to determine the cause.

      (1) Alarms must be assessed immediately by either the PF or by Central Alarm Station (CAS)/Secondary Alarm Station (SAS) personnel via Closed Circuit Television (CCTV).

      (2) CCTV assessment cameras used as primary assessment for PIDAS alarms must be fixed (i.e., not pan or tilt).

   c. Intrusion Detection System Monitoring. IDS must be monitored continuously by CAS/SAS personnel.

   d. Response Capability. Response capability to IDS alarms must be provided to protect safeguards and security (S&S) interests. PF response times must be compatible with the protection strategy employed at the site (e.g., as stipulated in Chapter II). The response capability must be provided by assigned PF personnel or by a local law enforcement agency (LLEA), as applicable.

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

(1) Each interior intrusion detection sensor must have a false and nuisance alarm rate of less than one alarm per 2,400 hours of operation, while maintaining proper detection sensitivity.

(2) Each exterior intrusion detection sensor must have a false and nuisance alarm rate of less than one alarm per 24 hours of operation, while maintaining proper detection sensitivity.

(3) If the alarms can be assessed at all times, either visually or by CCTV, a higher nuisance alarm rate may be tolerated if such alarms do not degrade system effectiveness. Although higher rates may be tolerated, each alarm occurrence, regardless of the cause, must be documented for analysis and trending purposes.

f. Performance. Systems, system components, and critical system elements must be performance-tested at a documented frequency commensurate with the requirements established in the DOE M 470.4-1, *Safeguards and Security Program Planning and Management*. 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.

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

2. INTERIOR INTRUSION DETECTION SYSTEM 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 inside Material Access Areas (MAA) and vault-type rooms must be installed to eliminate gaps in detection coverage.

(2) The IDS must be tested when installed and annually (at least every 12 months) thereafter.

(3) If testing indicates degradation of the IDS, it 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 IX.

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

e. Balanced Magnetic Switch (BMS) Intrusion Detection System. BMSs must initiate an alarm upon attempted substitution of an external magnetic field when the switch is in the normal secured position and whenever the leading edge of the door is moved 1 inch (2.5 cm) from the door jamb.

f. Volumetric Devices. Volumetric interior IDS 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 IDS must be functionally tested in accordance with locally established procedures at a documented frequency.

3. EXTERIOR INTRUSION DETECTION SYSTEM REQUIREMENTS. Exterior IDS are designed to detect unauthorized entry into security areas.

a. Exterior Intrusion Detection System. Exterior IDS must be designed with independent redundant data communication paths for protecting Category I and II quantities of SNM. The paths must be documented in a Site Safeguards and Security Plan (SSSP) or Site Security Plan (SSP), consistent with Table 1 (see Chapter VI).

b. Detection Capability. A PIDAS must be capable of detecting an individual crossing the detection zone by walking, crawling, jumping, running, or rolling, or climbing the fence at any point in the detection zone, with a detection probability of 90 percent and confidence level of 95 percent.

(1) The IDS must be tested when installed and annually (at least every 12 months) 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 XI, intrusion detection capabilities must be as effective as the rest of the perimeter IDS.

d. Perimeter Intrusion Detection Assessment System (PIDAS). PIDAS must be:

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

(2) located such that the length of each detection zone is consistent with the characteristics of the sensors used in that zone and the topography;

(3) designed, installed, and maintained to deter adversaries from circumventing 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.

(6) constructed in a manner that detects and deters the use of wire, piping, pulls, etc., that can not be eliminated from the isolation zone.

e. Perimeter Intrusion Detection and Assessment System Zone Degradation. Each PIDAS detection zone must be kept free of snow, ice, grass, weeds, debris, wildlife, and any other item that may degrade the effectiveness of the system. When this cannot be accomplished and detection capabilities become degraded, compensatory measures must be taken.

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.

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

(1) only be used as one of redundant or alternative paths. A hard-wired 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, hard-wired system used along with radio frequency is acceptable as a redundant communication path for temporary applications.

(2) 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) ensure the statement-of-health interval allows for an assessment and response.

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

(5) be capable of detecting and annunciating radio frequency jamming.

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

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

(8) use data encryption standards (DES) or other Government-approved encryption techniques for statement-of-health and alarm messages.

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

(10) have battery backup capabilities.

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

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

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

(14) provide for the activation of immediate compensatory measures if all or part of the system is being jammed, or if communications are otherwise lost, disrupted, or degraded.

(15) must provide communications in all weather conditions and provide immediate implementation of compensatory measures.

(16) lose no alarm data during the period of lost or degraded communications.

(17) ensure system integrity is maintained (i.e., not diminished) during multiple alarms.

b. 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 must 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 M 470.4-1, *Safeguards and Security Program Planning and Management*).

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

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

a. Protective Lighting–General. Protective system lighting must:

(1) enable assessment of unauthorized activities and/or persons at pedestrian and vehicular entrances and allow examination of DOE security badges and inspections of personnel, hand-carried items, packages, and vehicles.

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

(3) be positioned so that PF personnel are not spotlighted, blinded, or silhouetted by the lights; and the lighting placement and design should enhance, not minimize, PF night-vision capabilities.

(4) ensure the implementation of compensatory measures when the lighting system fails.

(5) 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 a minimum of 0.2-foot candle illumination within the PIDAS isolation zone.

(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.

6. ELECTRICAL POWER REQUIREMENTS. Power supply elements, located or operating within the confines of the site, must be protected from malicious physical attacks based on local site determination of vulnerability assessment (VA) impact. The requirements for primary and auxiliary power sources are as follows.

a. Primary Power Supply. All IDSs protecting Category I and II quantities of SNM and/or 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 required auxiliary power sources. The following power supply requirements apply:

(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/or 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) 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) Rechargeable batteries, when used, must be kept fully charged or subject to automatic recharging whenever the voltage drops to a level specified by the battery manufacturer. Non-rechargeable batteries must be replaced whenever their voltage drops 20 percent below the rated voltage or based on manufacturer's recommendations. An alarm signal must alert 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 (a minimum of 8 hours). Such power sources must have the necessary built-in features to facilitate periodic operational testing to verify their readiness.

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

CHAPTER VIII. ACCESS CONTROLS AND ENTRY/EXIT INSPECTIONS

1. GENERAL REQUIREMENTS. Personnel, hand-carried items, deliveries/mail, vehicles, and vehicle contents are subject to random inspections at security area boundaries except for Protected Areas (PA) and Material Access Areas (MAA), where inspections are mandatory. The cognizant security authority must approve local procedures that implement requirements for access control and entry/exit inspections. The following requirements apply to all security areas except Property Protection Areas (PPA).

   a. Access Control.

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

      (2) A person allowed to enter a Limited Area (LA), Exclusion Area (EA), PA, Vital Area, or MAA without an appropriate access authorization must be escorted at all times by an individual with:

         (a) knowledge of security procedures for the security areas to prevent compromise of classified information or matter;

         (b) appropriate access authorization;

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

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

   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 LAs and EAs is permitted. Authorized personnel are permitted to vouch for an individual, providing all access authorization and need-to-know requirements are met.

      (1) Personnel with the appropriate access authorization may vouch for another person with the required access authorization and need-to-know to "piggyback" (enter) an LA or EA.

      (2) Authorized personnel permitting the entry of another person 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 an LA, when protective force (PF)

personnel are not controlling access, are responsible and must ensure that unauthorized individuals do not enter ("piggyback").

(3) All personnel within a vehicle are required to produce DOE security badges when accessing an LA.

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

(1) Automated access controls used for access to any security area must 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). Badges must be validated by means of a PIN 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.

(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 Central Alarm Station (CAS) and Secondary Alarm Station (SAS) used to protect Category I and Category II quantities of SNM must monitor the automated access control system's intrusion alarm events.

(b) Electronic entry control point search equipment (e.g., metal detectors) may annunciate locally to a 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-carried 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 design 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 to meet site-specific criteria.

(3) Exits from security areas must satisfy life safety requirements of National Fire Protection Association (NFPA) 101, *Safety to Life from Fire in Buildings and Structures*. 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 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 barrier integrity.

(9) Entry control points must be located within the Perimeter Intrusion Detection Assessment System (PIDAS) and protected by the PIDAS when not in use. This configuration must provide a continuous PIDAS zone at the barrier that encompasses the entry control point.

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

(1) Prohibit entry until access is authorized.

(2) Permit entry of only one person at a time into PAs and MAAs.

(3) Control access when going from one security area into another security area with increased protection requirements.

(4) Perform entry and exit inspections to deter introduction of unauthorized personnel, prohibited and controlled articles, and unauthorized removal of S&S interests.

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 PA or MAA boundary), and when the personal identification number (PIN) or biometric system is either not working or not implemented, PF personnel must perform the access control requirements documented in the Site Safeguards and Security Plan (SSSP)/Site Security Plan (SSP).

c. Protection. Automated access control systems and associated equipment used to protect Category I and/or II quantities of SNM and/or classified matter must be protected.

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

(2) The system must record all attempts at access to include unsuccessful, unauthorized, and authorized.

(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.

(5) Records reflecting active assignments of DOE security badges, PINs, levels of access, access authorization, and similar system-related records must be maintained. Records of personnel removed from the system must be retained for 1 year, unless a longer period is specified by other requirements.

(6) Badge reader boxes, control lines, and junction boxes must have line supervision or tamper indication or be equipped with tamper resistant

devices. Field processors or multiplexers and other similar equipment must be tamper-alarmed or secured by a means that precludes surreptitious tampering with the equipment.

(7) Auxiliary power must be provided at installations where continuous operation is required.

4. ENTRY/EXIT INSPECTIONS. The following requirements apply to entry and exit inspections. The inspection process must be documented in the SSSP/SSP.

a. Inspection Program. An inspection program must ensure prohibited and controlled articles are detected before being brought into 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. Handheld and/or portable detectors, etc., must be available to resolve alarms and be available for use during inspection equipment failures. Inspection equipment can include metal detectors, special nuclear material (SNM) detectors, explosive detectors, and x-ray systems and must ensure that prohibited and controlled articles are detected before being brought into DOE facilities.

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

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

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

(5) Equipment must have both audible and visual alarms monitored by on-post PF 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-carried articles are subject to inspection before entry into a security area.

(1) Explosive Detection.

(a) Explosive detection equipment must ensure explosives are not introduced without authorization. The SSSP or SSP must document the analysis that establishes a facility's capability to

detect explosives and provides protection against the malicious use of explosives.

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

(c) Explosive detection systems must be able to detect low vapor-pressure explosives.

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

(2) Metal Detection. Metal detectors must ensure weapons are not introduced without authorization.

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

(b) Metal detectors used for MAA entry inspection must detect test weapons listed in paragraphs 4.b.(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. X-ray machines are used to reinforce and supplement metal detectors and protective personnel hand searches for prohibited and controlled articles.

(a) X-ray machines must provide a discernable image of prohibited and controlled articles.

(b) X-ray machines must image a 26 gauge wire at Step 5 of an American Society for Testing and Materials (ASTM) step wedge (see ASTM Standard F792-01).

(4) SNM Detectors. SNM detectors must meet the requirements described in the DOE M 470.4-6, *Nuclear Material Control and Accountability*. Note: Controls must be established to prevent unauthorized access to portal monitoring instrumentation and cabling.

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 classified matter or other S&S interests from security areas. Collocated SNM detectors and metal detectors must be used at PAs and/or MAAs to inspect personnel for SNM.

(1) Metal detectors used in the exit inspection process must ensure shielded SNM is not removed without authorization.

(2) SNM detectors used in the inspection process must ensure SNM is not removed without authorization.

CHAPTER IX. BARRIERS

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

   a. Barriers must be used to facilitate effective tactical and operational as well as economical use of protective force (PF) 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 be designed to provide a barrier resistant to bypass.

   c. Permanent barriers must be used to enclose security areas, except during construction or temporary 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 safeguards and security (S&S) interest being protected.

   e. 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 Property Protection Areas (PPAs).

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

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

      (1) Chain link fabric, consisting of a minimum of 11-gauge galvanized steel 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).

(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.

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

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

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

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

(3) 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.

(4) 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.

c. Temporary Security Fencing. During construction or temporary activities, 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) comply with site-specific protection goals and operational requirements.

3. PERIMETER BARRIER GATES.

a. Motorized Gates. Gate controls for motorized gates used for entry control points must be located within PF posts. 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.[a]

(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.

[a] For SNM, see Chapter X.

6. DOORS. Doors, door frames, and door jambs associated with walls serving as barriers must provide the necessary barrier delay required by the security plan. 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 National Fire Protection Association (NFPA) 101, *Safety to Life from Fire in Buildings and Structures*; 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/Mullions. An astragal/mullion must be used where doors used in pairs meet. Door louvers, baffles, or astragals/mullions, 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 (non-operable) 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 must meet the following requirements. Obscurants must consider spatial density versus time to deploy as determined by vulnerability assessment. 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. The potential adversary use of above-grade barriers for concealment should be considered when choosing an above ground vehicle barrier. Speed reducers should 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., non-removable hinge pins).

CHAPTER X. LOCKS AND KEYS

1. GENERAL REQUIREMENTS. A lock and key program must be established to ensure control and protection of nuclear weapons, weapon components, special nuclear material (SNM), high-value government assets, and classified matter.

2. LOCKS.

   a. Inventories must be conducted to ensure an accurate and up-to-date accountability of level I, II, and III security locks, keys, key rings, key ways, and pinned cores. Key locksets must meet American National Standards Institute (ANSI) Standard A156.2-1996, Grade 1, "Bored and Preassembled Locks and Latches," or ANSI A156.13-1996, Grade 1, "Mortise Locksets."

   b. 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.

   c. If a combination lock fails on any General Services Administration-(GSA)-approved security container or vault door, it must be repaired or replaced with a lock that meets Federal Specification FF-L-2740A, "Locks, Combination", before being used to protect classified matter or Categories I and II SNM. These failures must be documented and filed for future reference to assist in getting the problem corrected before future procurement of combination locks, (i.e., failed in the open or closed position and the reason for the failure).

   d. 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.

   e. Security 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) Lock bars must be 1¼ inches (31.75mm) by 3/16 inch (4.76mm), or equivalent, in cross section and constructed of material hardened to Rockwell C59 to C63 standards.

      (3) Hasps and yokes on repositories containing classified matter must be constructed of material hardened to Rockwell C59 to C63 standards; be at least ¼ inch (6.35mm) in diameter or equivalent cross section; and be secured to the repository by welding or riveting.

f. 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 Section B, DOE M 470.4-7, *Safeguards and Security Program References*.

g. Keys, key blanks, and key cutting codes must be protected in a graded fashion. Consideration must be given to the safeguards and security (S&S) interest being protected, the identified threat, existing barriers, and other protection measures afforded to the asset. Locks and keys must be categorized according to the asset being protected and an inventory and accountability system must be implemented.

(1) Security keys include mechanical keys, key cards, and access codes. Security keys do not include administrative or privacy lock keys to factory installed file cabinet locks, desk locks, toolboxes, etc. Access codes must be protected from compromise.

(2) Security key stock must be stored in a manner to prevent loss, theft, or unauthorized use. Personnel responsible for the control and issuance of locking systems and/or security keys must maintain an access authorization (security clearance) commensurate with that required for access to the asset(s) to which the key(s) provides direct access.

(a) The organization responsible for the pinning and cutting of Levels I, II, and III security locks and keys must report to the cognizant security authority.

(b) The pinning and cutting of Levels I, II, and III security locks and keys must be done within a Limited Area or have equivalent type protection measures.

(c) Grand master, master, sub-master, and control keys must be considered and analyzed in the vulnerability assessment process of the Site Safeguards and Security Plan (SSSP) or Site Security Plan (SSP).

(3) Security keys and locks are divided into four levels, Levels I through IV. Based on site analysis, line management must determine the appropriate key and lock level for application to the site.

(a) Level I security locks and keys must be used in the protection of nuclear weapons, weapon components, Category I quantities of SNM, Category II quantities of SNM that credibly roll-up to a Category I quantity, certain high value government assets, and Top Secret and/or Secret classified matter. Security key blanks must be restricted/proprietary; specifically, the blank must be unique to the site (e.g., does not use a commercially-available master key blank). Security locations such as vaults, vault-type rooms, material access

areas, SCIFs, and exclusion areas where Top Secret and/or Secret documents are stored require Level I security locks and keys.

(b) Level I security locks and keys, once put in service inside a Protected Area (PA), must not leave the PA without authorization. Assembled Level I security locks or cores and Level I security keys must remain under the direct control of an authorized person or must be stored in an approved GSA-approved repository or a vault-type room when not in use for the protection of the above assets (e.g., locksmith service work). Sites must conduct and document an assessment of duties for possible enrollment of locksmith personnel into the DOE Human Reliability Program (Title 10, Code of Federal Regulations, Part 712).

(c) The cognizant security authority must be notified within 8 hours if keys to doors/gates, or rooms that house S&S equipment is unaccounted for or determined to have been removed from the PA without authorization.

(d) Level I security locks, keys, key ways, and cores reported missing or discovered missing or in any way tampered with must be reported as an Incident of Security Concern These types of security incidents must be categorized as an Impact Measurement Index (IMI)-2 or IMI-3 event as identified in DOE M 470.4-1, *Safeguards and Security Program Planning and Management*.

(e) Any installation, replacement, or maintenance activities associated with Level I security locks must be documented to include the name of person who performed the activity.

(f) The number of Level I keys must be kept to an operational minimum.

(g) Level I keys must be maintained separately from all other keys on key rings and in key storage cabinets. Keys to storage cabinets must be in the physical possession of an authorized person or locked in a GSA-approved repository.

(h) All parts of broken Level I security keys must be recovered. If the functional part of the key (the blade) is lost or not retrievable, it must be considered a lost/missing key.

(i) Obsolete, damaged, or inoperative Level I keys must be destroyed and such destruction recorded. Keys must be destroyed in a manner authorized by the cognizant security authority.

(j) Risk assessments and identification of compensatory measures must be completed and documented on all Level I keys, so corrective actions can take place quickly after an incident.

(4) Level II security locks and keys are typically used for building doors, entry control points, gates in PA fences, exclusion area doors or other barriers or containers protecting Category II and Category III SNM as well as classified matter including documents classified at the Confidential level. All unused Level II security locks, keys, keyways and cores must be under direct control of an authorized person or stored in an approved GSA-approved repository or vault-type room. Incidents involving Level II keys must be reported as an IMI-3 as identified in the DOE M 470.4-1, *Safeguards and Security Program Planning and Management*.

(a) The number of Level II keys must be kept to an operational minimum.

(b) Level II locks and keys once put into service must not leave the facility without authorization.

(c) All parts of broken Level II security keys must be recovered. If the functional part of the key (the blade) is lost or not retrievable, it must be considered a lost/missing key.

(d) Obsolete, damaged, or inoperative Level II keys must be destroyed and such destruction recorded. Keys must be destroyed in a manner authorized by the cognizant security authority.

(5) Level III security lock and keys are typically on buildings, gates in fences, cargo containers, and storage areas for the protection of Government property. Level III security locks and keys must be used for the inside doors of buildings or office areas where Section A, Chapter II, 2. Classified Matter in Use, of DOE M 470.4-4, *Information Security*, is applicable.

(a) All parts of broken Level III security keys must be recovered. If the functional part of the key (the blade) is lost or not retrievable, it must be reported to the cognizant security authority.

(b) Obsolete, damaged, or inoperative Level III keys must be destroyed and such destruction recorded. Keys must be destroyed in a manner authorized by the cognizant security authority.

(c) Fabrication, issuance, return, and destruction of Level III security keys must be documented.

(d) Site specific procedures must be developed for control and accountability of Level III security keys and be approved by the cognizant security authority.

(6) Level IV locks and keys are typically used for offices where there is no open storage of classified matter and no classified matter in use. Desk, office and vehicle keys are considered administrative and have no control and accountability requirements.

h. An inventory system must be implemented to ensure the accountability of Levels I, II, and III security locks, keys, key rings, key ways, and pinned cores. Each accountable key and key core must have a unique identifying number placed on it. Cores will only be pre-pinned for the number required to fulfill the identified need. An inventory of pre-pinned cores will not be maintained for convenience.

(1) Fabrication, issuance, return, and destruction of Levels I, II, and III security keys must be documented. Grand master security keys must be kept to an operational minimum and under strict control. Duplicate and replacement keys must not have the same key number assigned as the key being replaced or duplicated. The inventory record must identify the specific duplicate and replacement keys. If replaced, the disposition of the key being replaced must be identified.

(2) Inventories must include locks, keys in possession of key holders, issuance stock, and keys assigned to key rings/key cabinets. Key rings must have a unique identifying number placed on the ring. Key rings should be of the tamper indicating type. The inventory system must:

(a) document each person issued a Level I security lock and key and the individual who issued the lock(s) and key;

(b) document the location of the lock(s) and keys;

(c) support the 100 percent inventory of Level I security locks and keys that must be performed on a semi-annual basis by the responsible organization; and,

(d) provide support in inventorying of Level I security keys not assigned to an individual (e.g., key rings, key cabinets, and keys issued on a temporary basis) that must be performed daily.

(3) When a Level I security key is unaccounted for, immediate notification must be made to the cognizant security authority, compensatory measures must be immediately initiated and an IMI-2 or IMI-3 incident of security concern inquiry must be completed. If the key cannot be located within 24 hours, the affected lock(s) must be changed.

(4) An annual inventory must be conducted to account for all Levels II and III locks and keys. If a Level III lock or key is discovered missing or tampered with, the incident must be reported through the Reporting Incidents of Security Concern process. These types of events should be categorized as IMI-4 incidents as identified in DOE M 470.4-1, *Safeguards and Security Program Planning and Management*, unless the cognizant security authority elevates the IMI categorization level.

(5) Level IV locks and keys have no inventory requirement.

(6) Sites should implement a training plan for key custodians and anyone having responsibility for a security key to ensure they understand their responsibilities for security key control and accountability.

(7) Sites must have documented plans for key turn-in when personnel or programs are terminating or moving from one program to another.

CHAPTER XI. SECURE STORAGE

1. GENERAL REQUIREMENTS. Safeguards and security (S&S) interests, to include special nuclear material (SNM), nuclear weapons, and classified information or matter, must be protected as specified in Chapter II.

   a. Secure Storage. S&S interests requiring secure storage must be placed in vaults, vault-type rooms, vault-type-room complexes, and/or General Services Administration (GSA)-approved security containers. A vault and/or vault-type room (VTR) or security container must be located within a Limited Area (LA) (see Chapter IV).

   b. Approved Combination Locks. All security containers placed into service after 7-14-94 must have a lock that meets Federal Specification FF-L-2740A.

   c. Access Controls. Access to vaults and VTR must be strictly controlled and based on an appropriate access authorization and need-to-know.

      (1) Persons without need-to-know and the appropriate access authorization must be escorted at all times.

      (2) Protective measures to mask classified matter must be used before visitors or cleared persons without need-to-know receive access.

      (3) Means of controlling access must be documented in a Site Safeguards and Security Plan (SSSP) or Site Security Plan (SSP).

      (4) Access controls at vaults and VTR must provide logging or recording of all personnel entries and exits, including visitors. Logged or recorded entries must include the identification/name and date/time of entry and exit.

         (a) In vaults and VTR where entering personnel are restricted from access (e.g., a foyer) to classified matter or SNM, logging entry and exit is not required.

         (b) The cognizant security authority may waive the requirement for repeated logging for those personnel whose office is located within the boundary of the vaults and vault-type rooms. Initial daily entry and final daily exit logging are required.

   d. Miscellaneous Openings. Any miscellaneous openings of a size and shape to permit unauthorized entry (larger than 96 square inches [619.2 square cm] in area and more than 6 inches [15.24 cm] in its smallest dimension) must be equipped with barriers such as wire mesh, 9-gauge expanded metal, or rigid steel bars at least 0.5 inches (1.3 centimeters) in diameter, welded vertically and horizontally

6 inches (15.24 centimeters) on center. The rigid steel bars must be securely fastened at both ends to preclude removal. Where wire mesh, expanded metal, or rigid steel bars are used, care must be taken to ensure classified matter within the vault cannot be removed with any type of instrument. The annular space between the sleeve and the pipe or conduit must be filled with wood, waterproof caulking, or similar material to show evidence of surreptitious removal.

2. VAULTS AND VAULT-TYPE ROOMS. The standards required for construction of vaults and VTRs, other than GSA-approved modular vaults, apply to all new construction, reconstruction, alterations, modifications, and repairs. The cognizant security authority must approve VTR 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 resist forced penetration. 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-cm) thick reinforced concrete, poured in place, with a minimum 28-day compressive strength of 2,500 pounds per square inch (17,237 kilopascal). 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 4.b. below.

c. Vault-Type Room Construction. The perimeter walls, floors, and ceiling must be permanently constructed and attached to one another. All construction must be done in a manner that provides visual evidence of unauthorized penetration. The following 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 their removal 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. 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 0.5-inch (1.3-m) bars no more than 6 inches (15.24 cm) apart, 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 must be translucent or opaque.

(b) During non-working 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 cm) 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 door louvers or baffle plates are used, they 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 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 per tile must be installed. 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. VTR complex barriers must meet the penetration resistance, intrusion detection, and access control requirements to be used for open storage of classified matter.

a. VTR 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 intrusion detection system (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 VTR complex before they are allowed to enter, or supplementary protective measures must be employed to shield the security interest from view.

b. VTR Complex General Requirements. The general requirements for a VTR 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. Intrusion Detection System 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 and vault-type rooms. IDS are required in some instances where certain types of containers are used to store classified matter. The IDS must be activated when the vault or vault-type room is unoccupied or the security container is unattended, i.e., the storage area must either be manned constantly or under the protection of an IDS.

   a. Vaults. Doors or openings allowing access into vaults must be equipped with IDS devices. A balanced magnetic switch (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. VTRs. 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 penetration of the vault-type room envelope, the unattended openings discussed in paragraph 8., Chapter XI, also must 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.

         (a) The cognizant security authority may require the installation of sensors in the false floor area (or ceiling) if the distance exceeds 6 inches (15.24 cm).

         (b) The asset under protection must be considered when not requiring the installation of sensors between the true floor (or ceiling) and the false floor (or ceiling).

      (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 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 (OF) 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 cognizant security authority 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 Federal Standard 809, "Neutralization and Repair of GSA Approved Containers," 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. Voice communications systems used for security purposes must provide intelligible voice communications in all security areas for all modes of operation and operating conditions. Security system transmission lines and data must be protected in a graded manner from tampering and substitution. The communications equipment must meet the following requirements:

   a. Redundant Voice Communications. Facilities protecting Category I and II quantities of special nuclear material (SNM) must have a minimum of two different voice communications technologies to link the Central Alarm Stations (CAS)/Secondary Alarm Station (SAS) to each fixed post and protective force (PF) duty location.

      (1) Alternative communications capabilities must be available immediately if the primary communications system fails. 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 so that type of failure, unit serial number, and equipment type can be compiled.

   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 CAS. 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 and the Office of Security or the Office of the Associate Administrator for Defense Nuclear 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 (see Chapter V) and PF communications. PF communications include the procedures and hardware that enable officers to communicate with each other.

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

(1) Protective Force Radio System Requirements. Radios must be equipped with digital encryption that complies with DOE M 200.1-1, *Telecommunications Security Manual*. PF 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. The application of digital encryption may be implemented on a graded basis. When the PF communications are converted to meet the Federal Communications Commission (FCC) narrow band frequency requirements, digital encryption must be included.

b. Alternative Means of Communication. Alternative 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.

c. Local Law Enforcement Agency (LLEA) Communication. CASs (and PF secure communications centers) must be equipped with radio and telephone channels for communication with LLEA. An alternative communications capability from a SAS must be provided if the primary station is compromised.

3. DURESS SYSTEMS. Facilities with Protected Areas, Material Access Areas, 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.

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

(1) Radios must have 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 alternative 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 operate for an 8-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 guide lines from vehicular traffic.

CHAPTER XIII. MAINTENANCE

1. GENERAL REQUIREMENTS. Security-related subsystems and components must be maintained in operable condition. 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 non-critical physical protection system elements (see DOE M 470.4-1, *Safeguards and Security Program Planning and Management*).

   a. Compensatory Measures. Compensatory measures must be implemented immediately when any part of the critical system element protecting Category I and II quantities of special nuclear material (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 non-critical system elements, the cognizant security authority must approve compensatory measure implementation procedures.

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

   d. Other Corrective Maintenance. Corrective maintenance procedures for protecting Category III and IV quantities of SNM, or Secret or Confidential matter must be approved by line management and prescribed in the site's operation procedures.

3. PREVENTIVE MAINTENANCE. Preventive maintenance must be performed on critical safeguards and security (S&S) related subsystems and components. Preventive maintenance must comply-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) Central Alarm Station and Secondary Alarm Station communications and display systems;

      (3) data and voice communications systems;

(4) protective force equipment;

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

(6) package and hand-carried items inspection equipment;

(7) vehicle access control and inspection equipment; and

(8) security and safety lighting systems.

b. Other Preventive Maintenance. Perimeter Intrusion Detection Assessment System, security area and other security lighting, and security system-related emergency power or auxiliary power supplies must be included in a preventive 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 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 the 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 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 safeguards and security interests.

   a. Signs. Signs listing prohibited and controlled articles, as stated in paragraphs 1.a. and b., Chapter IV, must be posted at security area entrances.

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

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 (42 U.S.C. 2278a) and as implemented by 10 Code of Federal Regulations (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 posting the regulations and penalties for violations.

      (2) Section 662 of the DOE 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) 41 CFR part 101-20.300 governs entry to public buildings and grounds under the charge and control of the General Services Administration.

   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 of the Atomic Energy Act of 1954 (42 U.S.C. 2278a) and/or Section 662 of the DOE Organization Act (42 U.S.C. 7270b).

(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 2.c. 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, administration, or in the custody of DOE must be published in the *Federal Register*. The notice is effective upon 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 by 14 inches (28 x 36 cm).

d. Notification to the Federal Bureau of Investigation (FBI). 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.

CHAPTER XV. DOE BADGE PROGRAM

1. GENERAL REQUIREMENTS. DOE security badges must be issued to and worn by all DOE and contractor personnel to gain access to DOE facilities with safeguards and security (S&S) interests and security areas. The DOE security badge or the Office of Science (SC) badges are the only formats to be used.

   a. DOE Security Badge. The following requirements apply:

      (1) Specifications for the DOE security badge and Local Site-Specific Only (LSSO) badge are identified in Appendix 1.

      (2) The DOE security badge will be accepted at all Departmental facilities. Individuals at SC facilities with an access authorization must be issued a DOE security badge to gain access to non-SC Departmental facilities.

      (3) Employee identification cards must not be substituted for the DOE security badge or the SC badge.

      (4) The SC badge is not authorized for access to Departmental facilities that require the DOE security badge.

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

2. DOE SECURITY BADGES. Facilities that use the SC 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 Federal and contractor employees for access to sites throughout the Department.

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

      (2) Badges must be issued by the organization/badging authority reporting to the Departmental element maintaining the badge holder's master personnel clearance files. As a matter of convenience, arrangements can be made between separate DOE organizations that would allow an office separate from the clearance holding office to issue the DOE security badge.

(3) DOE line management must prescribe local procedures for issuance, use, accountability, and return of DOE security badges.

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 badges, and other site-specific badges designed and implemented to meet local requirements.

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

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

(2) DOE line management must prescribe procedures for the design, issuance, use, accountability, and return of LSSO badges.

(a) The issuing authority must inform the badge recipient of limitations of badge use (e.g., the LSSO badges must be used at the issuing site).

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

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

(d) The LSSO badge may contain the individual's photograph.

(3) LSSO temporary and visitor badges may use the color representing the access authorizations and be usable in the site's automated access controls system (see Appendix 1-1, paragraph 2.b.). 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) 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 DOE line management.

(4) Individuals who have been issued an LSSO badge, who visit another site and need access to Limited Areas, Exclusion Areas, Protected Areas, and Material Access Areas or classified information, must submit DOE F 5631.20, "Request for Visit or Access Approval" (see DOE M 470.4-1, *Safeguards and Security Program Planning and Management*).

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

e. Foreign National Badges. Badges issued to foreign nationals must be as follows.

(1) Cleared Foreign Nationals. Cleared foreign nationals must be issued a DOE security badge. The difference between the cleared foreign national 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 foreign national must be issued by the organization/badging authority reporting to the DOE organization holding the foreign national's personnel clearance file. Cleared foreign nationals must adhere to the requirements in DOE O 142.3, *Unclassified Foreign Visits and Assignments,* dated 6-18-04 (see DOE M 470.4-1, *Safeguards and Security Program Planning and Management*).

(2) Uncleared Foreign Nationals. An LSSO badge must be issued to uncleared employees who are foreign nationals and whose official duties

require routine or regular access to DOE facilities. These badges must be red. The color red is reserved exclusively for uncleared, foreign national badges and must not be used for any other type of LSSO badge. Uncleared, foreign nationals must adhere to the requirements in DOE O 142.3, *Unclassified Foreign Visits and Assignments,* dated 6-18-04 (see DOE M 470.4-1, *Safeguards and Security Program Planning and Management*).

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

a. Issuance of Security Badges. DOE security badges must be issued to DOE and contractor employees who have been granted access authorizations and who require access to DOE security areas. These badges must be used and accepted at all other sites and facilities (see DOE M 470.4-5, *Personnel Security*).

b. Issuance with Special Nuclear Material (SNM) or Classified Access. Measures must be taken to ensure that a single individual cannot issue a security badge allowing unauthorized access into an area containing SNM or classified matter.

c. Issuer Clearance Level. Personnel with read/write access to systems containing records and information concerning badges, access authorizations, and access control authentication data must be cleared at the same level (L or Q) as the highest access authorization in the system data set. Sites should develop security plans to control access to security systems that maintain badging and clearance information.

d. Site Usage. A DOE security badge must be used and accepted as evidence of access authorization and must be accepted for admittance to security areas without 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.

e. Individual Requirements. DOE line management approves 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 authority 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 and as approved by DOE line management, when it is no longer valid or required.

(4) Surrendering or returning the DOE security badge when requested according to local procedures approved by DOE line management.

(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.)

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

f. 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 similar high levels of assurance that unauthorized persons will not be allowed access to security areas, facilities, classified matter, or other security interests.

g. 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 a 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 DOE cognizant 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 the need. 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.

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

i. 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.

j. Temporary and Visitor Badge Reuse. 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: 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. Losses should be reported commensurate with Section N of DOE M 470.4-1, *Safeguards and Security Program Planning and Management*.

6. DOE SECURITY BADGE VALIDATION. DOE line management approves local procedures for validation of the DOE security badge at access control points (e.g., by automation or protective force (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 VIII.

7. DOE SECURITY BADGE SPECIFICATIONS. The DOE Security Badge Specifications are described in Appendix 1.

APPENDIX 1. SECURITY BADGE SPECIFICATIONS

The purpose of Appendix 1 is to describe the DOE Security Badge Program and badge specifications. Appendix 1 contains Official Use Only information and has been issued separately from this Manual. A copy of Appendix 1 may be obtained by contacting the Program Manager, Protection Program Operations at 301-903-6209.

SECTION B—SAFEGUARDS AND SECURITY ALARM MANAGEMENT AND CONTROL SYSTEMS (SAMACS)

The requirements for Safeguards and Security Alarm Management and Control Systems (SAMACS) used in the protection of Category I and II quantities of SNM and installed and operational after January 1, 2008, are contained in Section B. Section B contains, Unclassified Controlled Nuclear Information, and will be issued separately from this Manual. A copy of Section B may be obtained by contacting the Program Manager, Protection Program Operations at 301-903-6209.

ALL DEPARTMENTAL ELEMENTS TO WHICH DOE M 470.4-2,
***Physical Protection*, 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 Representatives to the Defense Nuclear Facilities Safety Board
Office of Economic Impact and Diversity
Office of Electric Transmission and Distribution
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 Security and Safety Performance Assurance
Office of the Inspector General
Office of Intelligence
Office of Legacy Management
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 Worker and Community Transition
Office of Energy Assurance
Office of Energy Efficiency and Renewable Energy
Bonneville Power Administration
Southeastern Power Administration
Southwestern Power Administration
Western Area Power Administration

CONTRACTOR REQUIREMENTS DOCUMENT

DOE M 470.4-2, *PHYSICAL PROTECTION*

All requirements contained in DOE M 470.4-2, *Physical Protection*, apply to contractors who are responsible for operating and/or administering the Department of Energy (DOE), including the National Nuclear Security Administration (NNSA), Physical Protection Program for protecting safeguards and security (S&S) interests. The requirements in DOE M 470.4-2, *Physical Protection*, must be assigned to all subcontractors who have responsibilities for operating, administering, and/or protecting DOE S&S interests.

Regardless of the performer of the work, the contractor is responsible for compliance with these requirements. All requirements contained in DOE M 470.4-2, *Physical Protection*, apply to site/facility management contractors with responsibility for S&S interests at DOE and NNSA facilities. These requirements must be flowed down to all subcontractors with specific responsibilities for operating, administering, and/or protecting DOE S&S interests. For all other subcontracts, the contractor is responsible for flowing down these requirements to subcontracts at any tier to the extent necessary to ensure the contractor's compliance with the requirements. In doing so, the contractor shall not unnecessarily or imprudently flow down requirements to subcontracts. That is, the contractor shall (1) ensure that it and its subcontractors comply with these requirements to the extent necessary to ensure the contractor's compliance and (2) only incur costs that would be incurred by a prudent person in the conduct of competitive business.

A violation of the provisions of this directive to the safeguards or security of Restricted Data or other classified information may result in a civil penalty pursuant to subsection a. of section 234B, of the Atomic Energy Act of 1954 (42 U.S.C. 228b.). The procedures for the assessment of civil penalties are set forth in Title 10, Code of Federal Regulations, Part 824, *Procedural Rules for Assessment of Civil Penalties for Classified Information Security Violations*, (10 CFR Part 824).