

PHYSICAL PROTECTION



**NATIONAL NUCLEAR SECURITY ADMINISTRATION
Office of Defense Nuclear Security**

AVAILABLE ONLINE AT:
<http://www.nnsa.energy.gov>

INITIATED BY:
Office of Defense Nuclear Security

(This Page Intentionally Left Blank)

PHYSICAL PROTECTION

1. **PURPOSE.** This NNSA Policy implements the National Nuclear Security Administration (NNSA) security requirements and restrictions of the U.S. Department of Energy (DOE) for the physical protection of interests ranging from facilities, buildings, Government property, and employees to national security interests such as classified information, special nuclear material (SNM), and nuclear weapons. A graded approach for the protection of the lowest level of government property and layered to the most critical is described in this NNSA Policy. All physical protection programs, practices, and procedures developed within NNSA must be consistent with and incorporate the requirements of this NNSA Policy along with all national requirements (Atomic Energy Act of 1954, Executive Orders, United States Code [U.S.C.], *Code of Federal Regulations* (CFR), National Industrial Security Program, etc.).
2. **BACKGROUND.** This NNSA Policy (NAP) was developed using DOE M 470.4-2A, *Physical Protection Manual*, dated 7-23-09, as a baseline and is tailored to meet the programmatic needs of the NNSA. This NNSA Policy incorporates national-level requirements and most requirements as set by the Department. When establishing new requirements or deleting requirements, NNSA carefully measured the value of the requirements and perceived or actual threat to the protection and control of classified matter based on a risk management approach using DOE O 470.3B, *Graded Security Protection (GSP) Policy*, dated 8-12-08, and the costs of implementation. Defense Nuclear Security (DNS) worked closely with the DOE Office of Health, Safety, and Security (DOE/HSS) in developing this NAP. DNS will continue to work closely with the Departmental security policy office, as well as with Departmental inspection and oversight offices, in managing the NNSA security policy program. Some specific changes as outlined in this NNSA Policy include:
 - a. The term vault-type room (VTR) was replaced with the National Industrial Security Program Operating Manual term of closed areas (CAs). This change is due to operational necessity because it may be necessary to construct CAs for storage if General Services Administration (GSA)-approved containers or vaults are deemed unsuitable or impractical. The use of CAs within NNSA provides a level of security consistent with national standards and allows increased flexibility in storage of classified matter.
 - b. In coordination with the NNSA *Information Security* NAP, classified matter-in-use or “day-lock” procedures were restored into this NNSA Policy and are an acceptable, cost-effective way of protecting classified information in use during working hours. Day-lock benefits from layers of access control and security at NNSA sites and is a configuration virtually unpredictable for an adversary to exploit. Day-lock is a term used for classified matter-in-use during working hours and should not be confused with storage of classified matter. Day-lock requirements are contained in the NNSA *Information Security* NAP.
 - c. Prescriptive barrier design requirements were removed. By removing the elaborate details, barriers can serve their primary function as an area of

demarcation. The cognizant security authority (CSA) can now determine if a brick wall or other type of fencing meets the protection requirements necessary.

- d. Intrusion detection system (IDS) alarm coverage is allowed for engineered openings. By clearly defining an engineered opening and allowing for IDS protection, difficult construction issues can be averted without seeking deviations or installing volumetric alarms.
- e. Changes were made to the requirements for locks and keys. Level IV keys were deleted from this NNSA Policy because they are not considered security keys and the requirements for Level III keys were modified.
- f. The chapter on Safeguards and Security Alarm Management and Control Systems (SAMACS) was eliminated from this NNSA Policy. NNSA recommends that SAMACS be updated and incorporated as a technical standard, not a policy document. SAMACS outlined the requirements used in the protection of Category I and II quantities of SNM facilities installed and operational after January 1, 2008. These requirements, although outdated, still reside in DOE M 470.4-2A, where they can be referenced when necessary.

3. CANCELLATIONS.

- a. This NNSA Policy does not cancel any NNSA-issued policy. It does, however, replace DOE M 470.4-2A for application to the NNSA's Physical Protection Program.
- b. Cancellation of a Departmental policy (Policy, Order, Manual, or Notice) or NNSA policy does not, by itself, modify or otherwise affect any contractual obligation to comply with the policy. Canceled policies that are incorporated by reference in a contract remain in effect until the contract is modified to delete the references to the requirements in the canceled policies.

4. APPLICABILITY.

- a. All NNSA Elements. Except for the exclusion in paragraph 4d, this NNSA Policy applies to all NNSA elements. This NNSA Policy automatically applies to NNSA elements created after it is issued.
- b. NNSA Federal Employees. Except for the exclusion in paragraph 4d, this NNSA Policy applies to all NNSA Federal employees. All requirements identified in this NNSA Policy as solely a Federal function are individually identified.
- c. NNSA Contractors. Except for the exclusions in paragraph 4d, this NNSA Policy sets forth requirements that will apply to site/facility management contracts.
 - (1) This NNSA Policy must be included in the site/facility management contracts that involve classified matter or nuclear materials and contain

DOE Acquisition Regulation (DEAR) clause 952.204-2, *Security Requirements*.

- (a) NNSA elements must notify contracting officers of affected site/facility management contracts to incorporate this NNSA Policy into those contracts.
 - (b) Once notified, contracting officers are responsible for incorporating this NNSA Policy into the affected contracts via the laws, regulations, and DOE directives clause of the contracts.
 - (c) Requirements identified as solely a Federal function will not be incorporated into contracts.
- (2) A violation of the provisions of this NNSA Policy 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. 2282b). The procedures for the assessment of civil penalties are set forth in 10 CFR 824, *Procedural Rules for the Assessment of Civil Penalties for Classified Information Security Violations*.
- (3) As stated in DEAR clause 970.5204-2, *Laws, Regulations, and DOE Directives*, regardless of the performer of the work, site/facility contractors that have this NNSA Policy incorporated into their contracts are responsible for compliance with this NNSA Policy. Affected site/facility management contractors are responsible for flowing down the requirements of this NNSA Policy 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 NNSA Policy and only incur costs that would be incurred by a prudent person in the conduct of competitive business.
- (4) This NNSA Policy does not automatically apply to other than site/facility management contracts. Application of any of the requirements of this NNSA Policy to other than site/facility management contracts will be communicated as follows:
- (a) Heads of Field Elements and Headquarters NNSA Elements. Review procurement requests for new non-site/facility management contracts that involve classified matter or nuclear materials and contain DEAR clause 952.204-2, *Security Requirements*, and ensure that the requirements of this NNSA Policy are included in those contracts.

- (b) Contracting Officers. Assist originators of procurement requests who want to incorporate the requirements of this NNSA Policy in new non-site/facility management contracts, as appropriate.
- d. Exclusion. In accordance with the responsibilities and authorities assigned by Executive Order 12344, *Naval Nuclear Propulsion Program* codified at 50 U.S.C. sections 2406, 2511 and to ensure consistency throughout the joint Navy/DOE organization of the Naval Nuclear Propulsion Program, the Deputy Administrator for Naval Reactors (Director) will implement and oversee all requirements and practices pertaining to this NNSA Policy for activities under the Director's cognizance, as deemed appropriate.

For NNSA HQ elements which are resident at and serviced through DOE HQs, this NAP will not be applicable as the security servicing organization is the DOE Office of Health, Safety, and Security (HSS). NNSA will reevaluate the ability to and will be required to continue to follow all DOE policy, orders, and manuals.

5. AUTHORITIES.

- a. Title XXXII of Public Law 106-65, National Nuclear Security Administration Act, as amended, which established a separately organized agency within DOE.
- b. Secretary of Energy Delegation Order No. 00-003.00B to the Under Secretary for Nuclear Security, dated 1-22-10.

6. RESPONSIBILITIES.

- a. Under Secretary for Nuclear Security/Administrator, National Nuclear Security Administration.
 - (1) Has authority over, and is responsible for, all programs and activities of the NNSA. This authority includes, but is not limited to, strategic management, policy development and guidance, program management and direction, administration of contracts, and legal issues.
 - (2) Is responsible for the management and implementation of safeguards and security (S&S) programs administered by NNSA.
- b. NNSA General Counsel. Provides timely review and advice on all legal issues relating to the Physical Protection Programs of the NNSA.
- c. NNSA Contracting Officers.
 - (1) After notification by the appropriate program official, incorporate this NNSA Policy into affected contracts via the laws, regulations, and DOE directives clauses of the contracts.

- (2) Assist originators of procurement requests who want to incorporate this NNSA Policy in new non-site/facility management contracts, as appropriate.

d. Chief, Defense Nuclear Security (DNS).

- (1) Serves as the NNSA CSA responsible for the development and implementation of security programs and operations for facilities under the purview of NNSA including physical security, personnel security, materials control and accountability, classified and sensitive information protection, and technical security. NOTE: This authority may be delegated to subordinate NNSA line managers, and delegation must be documented in the appropriate safeguards and security management plan.
- (2) Oversees the security implementation of NNSA Special Access Programs and provides the NNSA portion of the DOE annual report to Congress.
- (3) Participates in international discussions regarding safeguards policies and procedures.
- (4) Issues direction for and oversees implementation of security conditions for operations under the cognizance of the NNSA.
- (5) Establishes a system of control measures to ensure that access to classified matter is limited to authorized persons. These control measures must be appropriate to the environment in which the access occurs and the nature of the matter. The system must include technical, physical, and personnel control measures.
- (6) Develops and allocates the NNSA security budget including budgets for the infrastructure that supports DNS missions.
- (7) Acts as the DOE representative for international S&S policy development including development of guidelines and technical documents and providing technical assistance.
- (8) Develops, manages, and maintains the North Atlantic Treaty Organization security policy for DOE.

e. NNSA Site Managers.

- (1) Implement the Physical Protection Program as the NNSA CSA for their specific site.
- (2) Re-delegate authorities as necessary to ensure the effective management of the Physical Protection Program unless specifically disallowed.

7. SUMMARY. This NNSA Policy consists of 13 chapters and one attachment that provide direction and requirements for planning, implementing, and monitoring the application of physical protection measures. The chapters describe the procedures and management process applicable to NNSA operating environments. Implementation of these procedures should be accomplished under an approved security plan, as described in DOE M 470.4-1, Chg. 1, which describes an integrated, performance-based approach to site security.
8. DEVIATIONS. Deviations from national regulations, including CFR and national-level policies, are subject to the deviation process of the governing document rather than the Departmental deviation process. This NNSA Policy conveys no authority to deviate from law or other national-level requirements.
 - a. Requests for deviations from requirements specific to the Department of this NNSA Policy must be processed in accordance with the provisions of DOE M 470.4-1, Chg. 1, *Safeguards and Security Program Planning and Management*, dated 3-7-06.
 - b. Protection of some national security interests cannot be accomplished by use of the measures defined in this NAP. In such unique circumstances, the appropriate cognizant security authority may approve protection requirements tailored to that particular interest using graded protection measures described in a specific security plan.
9. DEFINITIONS. Definitions for most terms included in the NNSA DNS S&S Program may be found in DOE M 470.4-7, *Safeguards and Security Program References*, dated August 26, 2005, but may also be included in this NNSA Policy if required for context. Other pertinent definitions are as follows:
 - a. Cognizant Security Authority. 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.
 - (1) NNSA Cognizant Security Authority (NNSA CSA). The Federal CSA responsible for inherently government functions and risk acceptance for security requirements that cannot be further delegated to the contractor.
 - (2) Cognizant Security Authority (CSA). The CSA at the contractor level. This is the level of authority granted to the contractor.
 - b. Closed Areas (CA). An area that meets the requirements of this NNSA Policy for safeguarding classified matter and/or a security interest that, because of its size, nature, or operational necessity, cannot be adequately protected by the normal safeguards or stored during nonworking hours in approved containers.
 - c. Day-lock. A practice that permits users to temporarily leave classified matter in areas where access is controlled and limited to individuals with appropriate

clearance and need-to-know as documented and prescribed by the CSA. Refer to NNSA *Information Security* NAP for additional day-lock requirements.

- d. Engineered Openings. Openings greater than 96 inches square that have been designed and constructed to allow access to storage locations for lawful purpose. Examples include, but are not limited to, door openings, window openings, and ventilation openings.
- e. Supplemental Protection. Supplemental protection measures include additional security measures such as GSA approved security containers, intrusion detection systems, protective force (PF) patrols, special checks or access control systems. Supplemental protection measures should be documented in the Site Security Plan (SSP) and approved by the CSA.

NOTE: GSA-approved security containers and approved vaults secured with a locking mechanism meeting Federal Specification FF-L-2740 do not require supplemental protection when the CSA has determined that the GSA-approved security container or approved vault is located in an area of the facility with security-in-depth.

NOTE: When PF are authorized, the schedule of patrol is 2 hours for Top Secret matter and 4 hours for Secret matter.

- 10. REQUIREMENTS. Detailed requirements are included in each section of this NNSA Policy.
- 11. REFERENCES.
 - a. References commonly used in the S&S Program are located in DOE M 470.4-7.
 - b. Title XXXII Public Law (P.L.) 106-65, National Nuclear Security Administration Act, as amended, which established a separately organized agency within the DOE.
 - c. *National Industrial Security Program Operating Manual* reissued February 28, 2006.
- 12. IMPLEMENTATION. Requirements that cannot be implemented within six months of the effective date of this NNSA Policy or within existing resources must be documented by the CSA and submitted to the Under Secretary for Nuclear Security/Administrator, NNSA through the NNSA CSA. A courtesy copy will be sent to the DOE Office of Health, Safety and Security. The documentation must include timelines and resources needed to fully implement this NNSA Policy. The documentation must also include a description of the vulnerabilities and impacts created by delayed implementation of the requirements.

13. CONTACT. Questions concerning this NNSA Policy should be addressed to the Director, Office of Field Support (NA-72), National Nuclear Security Administration, Office of Defense Nuclear Security, 1000 Independence Avenue SW, Washington, DC 20585.

BY ORDER OF THE ADMINISTRATOR:

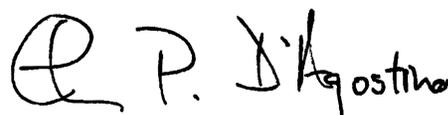

THOMAS P. D'AGOSTINO
Administrator

TABLE OF CONTENTS

PHYSICAL PROTECTION	i
1. Purpose	i
2. Background.....	i
3. Cancellations.....	ii
4. Applicability	ii
5. Authorities	iv
6. Responsibilities.....	iv
7. Summary.....	vi
8. Deviations	vi
9. Definitions	vi
10. Requirements	vii
11. References.....	vii
12. Implementation.....	vii
13. Contact.....	viii
CHAPTER I . PROTECTION PLANNING	I-1
1. General Requirements	I-1
2. Planning	I-1
CHAPTER II . SECURITY AREAS	II-1
1. General Requirements	II-1
2. General Access Areas (GAAs).....	II-1
3. Property Protection Areas (PPAs)	II-1
4. Limited Areas (LAs).....	II-1
5. Exclusion Areas (EAs)	II-3
6. Protected Areas (PAs).....	II-4
7. Material Access Areas (MAAs)	II-5
8. Special Designated Security Areas	II-6
CHAPTER III . PROTECTION OF CATEGORY I, II, III AND IV SPECIAL NUCLEAR MATERIAL (SNM) AND PROTECTION OF NUCLEAR WEAPONS AND COMPONENTS	III-1
1. General Requirements for the Protection of Category III and IV Special Nuclear Material	III-1
2. Category IV Quantities of SNM.....	III-1
3. Category III Quantities of SNM	III-1

4.	General Requirements for Category I and II Special Nuclear Material	III-1
5.	Category II Quantities of SNM	III-2
6.	Category I Quantities of SNM.....	III-2
CHAPTER IV . POSTING NOTICES.....		IV-1
1.	General Requirement	IV-1
2.	Prohibited and Controlled Articles	IV-1
3.	Surveillance Equipment.....	IV-2
4.	Trespassing	IV-2
CHAPTER V . LOCKS AND KEYS		V-1
1.	General Requirements	V-1
2.	Categories	V-1
3.	Lock and Key Standards	V-1
4.	Inventory.....	V-3
5.	Level I Security Keys and Locks.....	V-4
6.	Level II Security Keys and Locks	V-5
7.	Level III Security Keys and Locks	V-6
CHAPTER VI . TESTING AND MAINTENANCE		VI-1
1.	General Requirements	VI-1
2.	Lifecycle Planning.....	VI-1
3.	Maintenance.....	VI-1
4.	Testing	VI-2
5.	Established Testing Criteria.....	VI-3
6.	Testing and Maintenance Personnel Security Clearances	VI-5
7.	Record Keeping	VI-5
CHAPTER VII . BARRIERS		VII-1
1.	General Requirements	VII-1
2.	Penetration of Security Area Barriers.....	VII-1
3.	Hardware.....	VII-2
4.	Fencing	VII-2
5.	Perimeter Barrier Gates	VII-3
6.	Exterior Walls.....	VII-3
7.	Ceiling and Floors.....	VII-4
8.	Doors.....	VII-4
9.	Windows.....	VII-4

10. Protective Force Posts.....	VII-4
11. Utility and Other Barrier Penetrations and Openings.....	VII-5
12. Penetration of Security Area Barriers.....	VII-5
13. Barriers-Delay Mechanisms	VII-6
14. Activated Barriers, Deterrents, and Obscurants	VII-6
15. Vehicle Barriers.....	VII-6

CHAPTER VIII . COMMUNICATIONS, ELECTRICAL POWER AND LIGHTINGVIII-1

1. Communications.....	VIII-1
2. Electrical Power.....	VIII-4
3. Electrical Power for CAT I and II Facilities.....	VIII-4
4. Lighting.....	VIII-5
5. Lighting.....	VIII-6

CHAPTER IX . SECURE STORAGE.....IX-1

1. General Requirements	IX-1
2. Vaults and Closed Areas.....	IX-1
3. Closed Area Room Complex	IX-4
4. Intrusion Detection Systems.....	IX-4
5. Security Containers.....	IX-5
6. Non-Conforming Storage	IX-6

CHAPTER X . INTRUSION DETECTION AND ASSESSMENT SYSTEMS..... X-1

1. General Requirements	X-1
2. Interior IDS Requirements.....	X-2
3. Exterior IDS Requirements	X-2
4. Radio Frequency Alarm Communications	X-2
5. Protection of IDSs.....	X-2
6. General Requirements for Category I and II Quantities of SNM.....	X-6
7. Perimeter Intrusion Detection System	X-7

CHAPTER XI . ALARM MANAGEMENT AND CONTROL SYSTEMS.....XI-1

1. General Requirements	XI-1
2. Alarm Stations	XI-1
3. Commercial Alarm Stations	XI-1
4. General Requirements for the Protection of Category I and II SNM.....	XI-2
5. Closed-Circuit Television (CCTV) System.....	XI-2

CHAPTER XII . ENTRY/EXIT SCREENING XII-1

- 1. General.....XII-1
- 2. Entry InspectionsXII-1
- 3. Exit InspectionsXII-2

CHAPTER XIII . PROTECTION DURING TRANSPORTATIONXIII-1

- 1. General Requirements XIII-1
- 2. Category IV Quantities of SNM..... XIII-1
- 3. Category III Quantities of SNM XIII-1
- 4. Offsite Shipment..... XIII-2
- 5. Onsite Shipments XIII-2

ATTACHMENT 1 – DOE SECURITY BADGE PROGRAM.....1

- 1. General Requirements1
- 2. Type of DOE Badge1
- 3. Issuance, Use, Recovery, and Destruction of DOE Security & LSSO Badges4
- 4. Accountability of DOE Security Badges6
- 5. Protection of DOE Badge Materials and Equipment.....6
- 6. DOE Security Badge Validation.....7
- 7. DOE Security Badge Recipient Requirements7
- 8. DOE Security Badge-HSPD-12 Requirements7

Chapter I - PROTECTION PLANNING

1. GENERAL REQUIREMENTS. This National Nuclear Security Administration (NNSA) Policy establishes requirements for the physical protection of all NNSA interests including NNSA property and national safeguards and security interests under U.S. Department of Energy (DOE) purview. Interests requiring protection range from Government facilities, buildings, property and employees, to national security interests such as classified information, special nuclear material (SNM) and nuclear weapons. Physical protection strategies must be developed, documented, and implemented consistent with the DOE O 470.3B, *Graded Security Protection (GSP) Policy*, dated 8-12-08 formerly the *Design Basis Threat Policy*, and national policy to protect against radiological, chemical, or biological sabotage.
2. PLANNING. The implementation of graded physical protection programs required by this NNSA Policy must be systematically planned, executed, evaluated, and documented as described by a Site Security Plan (SSP) (see DOE M 470.4-1, Chg. 1, *Safeguards and Security Program Planning and Management*, dated 3-7-06).
 - a. Physical protection programs must be based on the most recent GSP information and used in conjunction with local threat guidance.
 - b. Departmental interests must be protected from malevolent acts such as theft, diversion, and sabotage and events such as civil disorder by considering site and regional threats, protection planning strategies, and protection measures.
 - c. SNM must be protected at the higher level when roll-up to a higher category can occur within a single security area unless the facility has conducted an analysis that determined roll-up was not credible (see DOE M 470.4-6, Chg. 1, *Nuclear Material Control and Accountability*, dated 8-14-06, and DOE M 470.4-7, *Safeguards and Security Program References*, dated 8-26-05).
 - d. Sites upgrading security measures must consider the benefits provided using security technology by conducting life-cycle cost-benefit analyses comparing the effectiveness of security technology to traditional manpower-based methodologies. However, at Category I and Category II facilities various manpower alternatives to include security technologies must be used to allow protective force personnel to concentrate on the primary mission of protecting nuclear weapons, SNM, and designated high-value targets.
 - (1) If parking areas are near security areas and could interfere with intrusion detection sensor fields, clear zones, protective force operations, or pose a threat to target areas, these parking issues must be addressed in the SSP.
 - (2) Parking areas must not impact security equipment, security operations or be located in manner that degrades protection of Departmental interests.

- (3) Vehicle bomb threats must be considered in determining the location of vehicle parking areas. For all new construction, parking areas should be located at a pre-determined distance from buildings to minimize a vehicle bomb threat. The set-back distance must be determined by using the GSP and site vulnerability assessment.

Chapter II - SECURITY AREAS

1. GENERAL REQUIREMENTS. Security areas are established to provide protection to a wide array of safeguards and security (S&S) interests under the U.S. Department of Energy's (DOE) purview, to include nuclear weapons, special nuclear material (SNM), classified information, buildings, facilities, Government property, employees and other interests. The security areas described in this Chapter address a graded approach for the protection of S&S interests.
2. GENERAL ACCESS AREAS (GAAs). GAAs may be established to allow access to certain areas with minimum security requirements as determined by the cognizant security authority (CSA). These designated areas are accessible to all personnel including the public. The CSA should establish security requirements for those areas designated as a GAA.
3. PROPERTY PROTECTION AREAS (PPAs). PPAs are security areas that are established to protect employees and Government buildings, facilities and property.
 - a. General Requirements. 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. The CSA must designate, describe, and document PPA protection measures within their Site Security Plan (SSP).
 - b. Signs. See Chapter IV of this National Nuclear Security Administration (NNSA) Policy.
 - c. Access Control. Access controls must be implemented as established by the CSA.
 - d. Inspection Program. An inspection program is to deter prohibited and controlled articles from being brought into PPA facilities and deter unauthorized removal of government assets. All personnel, vehicles, packages, and hand-carried articles are subject to inspection before entering or exiting a security area.
 - e. Visitor Processing. Site-specific requirements and procedures for receiving visitors must be developed and approved by the CSA.
4. LIMITED AREAS (LAs). LAs are security areas designated for the protection of classified matter and Category III SNM. Specific protection requirements applicable to Category III quantities of SNM are provided in Chapter III.
 - a. General Requirements. LA boundaries are defined by physical barriers encompassing the designated space and access controls.
 - b. Access Control. The identity and clearance level of each person seeking entry to an LA must be validated by protective force (PF), or other appropriately authorized personnel, or by an automated system and documented in the SSP.

- c. Inspection Program. An inspection program is to deter prohibited and controlled articles from being brought into LA facilities and deter unauthorized removal of government assets. All personnel, vehicles, packages, and hand-carried articles are subject to inspection before entering or exiting a security area.
- d. Personnel Access. Individuals without a security clearance must be escorted by an authorized person who is to ensure measures are taken to prevent a compromise of classified matter.
 - (1) Escort Ratios. The CSA must establish escort-to-visitor ratios in a graded manner for each LA or above security area.
 - (2) Escort Responsibilities. Any person permitted to enter a LA or above who does not possess a security clearance at the appropriate level must be escorted at all times by an appropriately cleared and knowledgeable individual trained in local escort procedures.
 - (a) Escorts must ensure measures are taken to prevent compromise of S&S interests.
 - (b) The escort must ensure the visitor has a need-to-know for the security area or the S&S interests. Need-to-know requirements are defined in the NNSA *Information Security* NAP.
 - (3) Access Validation. Validations must occur at entry control points of LAs.
 - (a) The identity and security clearance held by each person seeking entry must be validated by appropriately authorized personnel, automated systems, or other means documented in the SSP.
 - (b) Where practicable, PF personnel will not be used to control access to LAs.
 - (4) “Piggybacking.” The following requirements must be documented in the SSP if piggybacking into LAs is permitted.
 - (a) Personnel with the appropriate security clearance may vouch for another person with the required security clearance to “piggyback” into an LA.
 - (b) 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 security clearance identifier on the badge. When PF personnel are not controlling access to the LA, the federal or contractor employee authorized to enter the LA is responsible for ensuring that those accompanying individuals are authorized entry.

- (5) Automated Access Control Systems. Automated access control systems may be used if the following requirements are met.
 - (a) Automated access controls used for access to a LA security area must verify that the DOE security badge is valid (i.e., that the badge data read by the system match the data assigned to the badge holder).
 - (b) Personnel or other protective measures are required to protect 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 that the data are protected in accordance with the SSP.
 - (c) The system must record all attempts at access to include unsuccessful, unauthorized, and authorized.
 - (d) Door locks opened by badge readers must be designed to relock when the door has closed.
 - (e) Transmission of security clearance and personal identification or verification data between devices/equipment must be protected in accordance with the SSP.
 - (f) Records reflecting active assignments of DOE security badges, security clearance, 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. Personal data must be protected in conformance with the Privacy Act, (see 5 U.S.C. 552).
- e. Visitor Processing. Site-specific requirements and procedures for receiving visitors must be developed and approved by the CSA.
- f. Vehicle Access. Vehicle access requirements will be documented in the SSP.
- g. Signs. See Chapter IV of this NNSA Policy.
5. EXCLUSION AREAS (EAs). EAs are established to protect classified matter where 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 and be located within the minimum of an LA.
 - b. Access Control. In addition to the requirements for an LA, the following requirements apply to access to an EA. Visitor logs must be used for EAs.

- c. Inspection Program. An inspection program is to deter prohibited and controlled articles from being brought into EA facilities and deter unauthorized removal of government assets. All personnel, vehicles, packages, and hand-carried articles are subject to inspection before entering or exiting a security area.
 - d. Intrusion Detection. When the exclusion area is unoccupied and classified matter is not secured in a security container the EA must, at a minimum, meet the requirements of a closed area or an appropriate level of protection as determined by the CSA.
6. PROTECTED AREAS (PAs). PAs are security areas that are established to protect Category II or greater quantities of SNM and may also contain classified matter. The PA provides concentric layers of security for the material access area (MAA). In addition to meeting LA requirements, the following apply to a PA.
- a. General Requirements. PAs must be encompassed by physical barriers that identify the boundaries, surrounded by a perimeter intrusion detection and assessment system (PIDAS), and equipped with access controls that ensure only authorized personnel are allowed to enter and exit. Entry control points must be located within the 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. The entry control point should permit entry of only one person at a time into PAs. Electronic entry control point search equipment (e.g., metal detectors) must annunciate locally to a PF-staffed entry control point.
 - b. Inspection Program. An inspection program must be able to detect prohibited and controlled articles before they are brought into PA facilities. All personnel, vehicles, packages, and hand-carried articles are subject to inspection before entry into a security area. Likewise, such programs must be able to detect removal of S&S interests. An inspection program must be established by the CSA and documented in the SSP.
 - c. Access Control. When the personal identification number (PIN) or biometric system is either not working or not implemented at security areas requiring measures in addition to access control (e.g., at a PA or MAA boundary), PF or other trained security personnel must perform the access control requirements as documented in the SSP.
 - (1) Personnel Access. Unescorted access must be controlled to limit entry to individuals with an L or Q security clearance.
 - (a) Visitor logs or automated access control logs must be used for PAs.
 - (b) Validation of the security clearance must occur at PA entry control points.

1. The identity and security clearance of each person seeking entry must be validated by PF personnel or
 2. Automated access control systems may be used in place of or in conjunction with protective force personnel to meet access requirements.
- (c) Both the Central Alarm Station (CAS)/Secondary Alarm Station (SAS) must monitor the unattended automated access control system's intrusion alarm events.
- (d) Badge readers at PAs must have anti-passback protection for unattended automated access control.
- (e) If PA access is controlled by an unattended automated access control system, the system must verify the following:
1. a valid DOE security badge (badge validation must match the data assigned to the badge holder),
 2. valid security clearance, and
 3. valid PIN or
 4. valid biometric.
- (2) Vehicle Access. Private vehicles are prohibited. Government-owned or Government-leased, service or vendor 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.
- (3) Visitor Processing. Site-specific requirements and procedures for receiving visitors must be developed and approved by the CSA.
7. MATERIAL ACCESS AREAS (MAAs). MAAs are security areas established to protect Category I quantities of SNM. In addition to requirements for a PA, the following apply to an MAA. The entry control point should permit entry of only one person at a time into MAAs.
- 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 and must have distinct boundaries. Multiple MAAs may exist within a single PA; however, an MAA cannot cross a PA boundary. MAAs may be co-located with the PA boundary if

documented in the SSP and protection values meet those identified in the vulnerability assessment.

- (2) While an MAA is required for the protection of Category I quantities of SNM, classified matter may exist within an MAA with CSA approval. In such instances, the MAA constitutes adequate protection of open storage of classified matter for Secret and below.
- b. Access Control. Access control must be administered by armed PF personnel and/or automated access control systems.
- (1) Badge readers at MAAs must have anti-passback protection for unattended automated access control.
 - (2) Access must be controlled to limit entry to individuals with a Q security clearance who have been authorized for entry consistent with need-to-know and operations.
 - (3) Individuals without appropriate security clearance must be escorted.
 - (a) The CSA must establish escort-to-visitor ratios for the MAA.
 - (b) The escort must ensure measures are taken to prevent compromise of classified matter or access to SNM.
 - (4) Validation of security clearance and other access requirements as documented in the SSP must occur at MAA entry control points.
 - (5) Site-specific requirements and procedures for visitors must be developed and approved by the CSA. The procedures must provide for the information described in Attachment 1.
8. SPECIAL DESIGNATED SECURITY AREAS. Other areas such as Sensitive Compartmented Information Facilities, Special Access Program Facilities, secure communications centers, and automated information system centers will be protected in accordance with applicable Standards.

**Chapter III - PROTECTION OF CATEGORY I, II, III AND IV
SPECIAL NUCLEAR MATERIAL (SNM) AND PROTECTION OF NUCLEAR
WEAPONS AND COMPONENTS**

1. GENERAL REQUIREMENTS FOR THE PROTECTION OF CATEGORY III AND IV SPECIAL NUCLEAR MATERIAL (SNM). This Chapter contains the requirements for protecting Category I, II, III and IV quantities of 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, parts, or explosives that are classified must receive the physical protection required by the higher level of classification or category of SNM, whichever is the more stringent.
2. CATEGORY IV QUANTITIES OF SNM. The following requirements apply.
 - a. In Use or Processing. Category IV quantities of SNM must be used or processed within at least a property protection area and in accordance with local security procedures approved by the cognizant security authority (CSA).
 - b. Storage. Category IV quantities of SNM must be stored in a locked area within at least a property protection area, and procedures must be documented in an approved Site Security Plan.
3. CATEGORY III QUANTITIES OF SNM. The following requirements apply.
 - a. In Use or Processing. Category III quantities of SNM must be used or processed in an access controlled security area within at least a limited area (LA) and in accordance with local security procedures approved by the CSA.
 - 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 intrusion detection system or Protective Force (PF) patrol physical check at least every 8 hours.
4. GENERAL REQUIREMENTS FOR CATEGORY I AND II SNM. This section defines requirements for protecting nuclear weapons, components, and Category I and II quantities of SNM. SNM must be protected at the higher level when roll-up to Category I quantities can occur within a single security area unless the facility has conducted an analysis that determined roll up was not credible. The policy cited in this section applies to fixed facilities and sites within a designated Protected Area (PA) or Material Access Area (MAA) and not the conduct of onsite movement of SNM or operations managed by the Office of Secure Transportation (OST). The OST is responsible for the promulgation of specific internal guidance governing the protection afforded all U.S. Department of Energy (DOE) matter entrusted to OST for transport by surface and air. Transportation of SNM, whether onsite or by OST, must be provided protection equivalent to that provided by fixed sites for the same material.

- a. A facility must not possess, receive, process, transport, or store nuclear weapons or SNM until that facility has been cleared (see DOE M 470.4-1, Chg. 1, *Safeguards and Security Program Planning and Management*, dated 3-7-06).
- 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. SNM, parts, explosives or munitions that are classified must receive the physical protection required by the highest level of classification or category of SNM, whichever is the more stringent.

5. CATEGORY II QUANTITIES OF SNM.

- 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 closed area located within a PA.

6. CATEGORY I QUANTITIES OF SNM.

- a. In Use or Processing. Category I quantities of SNM must be located within a MAA. Any MAA containing unattended Category I quantities of SNM must be equipped with an intrusion detection system or detection must be provided by PF.

Storage. Category I SNM must be stored in a vault or in a closed area with enhanced protection measures. The performance of the integrated protection system, including storage areas, for Category I SNM must include sufficient detection, assessment, and response capabilities to provide a high system's effectiveness against threats outlined in the Department's Graded Security Protection policy.

Chapter IV - 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.
2. PROHIBITED AND CONTROLLED ARTICLES. Signs listing prohibited articles must be posted at the outermost security area boundary. Additional prohibited and controlled article signs may be posted at inner security areas [Property Protection Area, Limited Area (LA), Exclusion Area (EA), Protected Area (PA), and/or Material Access Area (MAA)] as determined by the cognizant security authority (CSA). The listing of controlled articles is to be prepared by the sites.

Authorization for prohibited articles to be used for official Government business must be documented in a Site Security Plan (SSP). The articles listed below will not be permitted onto U.S. Department of Energy (DOE) property without appropriate authorization.

a. Prohibited Articles. Prohibited articles include items such as:

- (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) other items prohibited by law. Specific information covering prohibited items may be found under the provisions of 10 *Code of Federal Regulations* (CFR) Part 860 and 41 CFR Part 102-74 Subpart C.

b. Controlled Articles.

- (1) Controlled articles such as portable electronic devices, both Government and personally owned, capable of recording information or transmitting data (e.g., audio, video, radio frequency, infrared, and/or data link electronic equipment) are not permitted in LAs, EAs, PAs, and MAAs, without prior approval. The approval process must be documented in the SSP. NOTE: Government-owned computer systems that are part of the day-to-day operations are exempt from the requirement. The CSA must specify any other equipment to be exempted from the approval process.
- (2) Sites are to develop procedures to account for, control, and limit all controlled articles entering specified security areas. These procedures must be approved by the CSA.

- (a) For application to Special Access Program Facilities (SAPFs), Sensitive Compartmented Information Facilities, etc., the Director Central Intelligence Directive (DCID) 6/9 and DCID manual, *Physical Security Standards for Sensitive Compartmented Information Facilities*, program guidance must be implemented.

For SAPFs, the programmatic policy addressing Controlled Articles would be issued by the Special Access Program Administrator (see DOE M 471.2-3B, *Special Access Program Policies, Responsibilities, and Procedure*, dated 10-29-07).

- (b) Office of Secure Transportation Federal Agents, DOE protective personnel, and other Federal agents and local law enforcement officials with jurisdiction whose duties routinely require the carrying and operation of controlled articles, are exempt from this requirement unless a nuclear safety reason exists to prohibit certain communication devices; e.g., cellular telephones, transceiver-radios, and other electronic radiating/emitting devices. If such a prohibition exists, it is to be documented in specific agreements between the site and Federal agency.

3. SURVEILLANCE EQUIPMENT. Warning signs and/or notices must be posted at entrances to areas under electronic surveillance advising that physical protection surveillance equipment is in operation.
4. TRESPASSING. Signage indicating DOE property must be posted according to statutes, regulations, and the administrative requirements for posting specified in this National Nuclear Security Administration (NNSA) Policy.
 - a. Statutory and Regulatory Provisions:
 - (1) Section 229 of the Atomic Energy Act of 1954 (42 U.S.C. 2278a) as implemented by 10 CFR 860, prohibits unauthorized entry and unauthorized carrying, transporting, or otherwise introducing or causing to be introduced any dangerous 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) Public Law 80-566 (Title 40, U.S. Code 318); and Public Law 81-152 provide the rules and regulations governing public buildings and grounds under the charge and control of the General Service Administration (GSA). 41 CFR 102-74 Subpart C governs entry to public buildings and grounds under the charge and control of the GSA.
- (4) Signs prohibiting trespassing must be conspicuously posted at all entrances of each designated facility, installation or parcel or real property and at such intervals along the perimeter as will provide reasonable assurance of notice to persons about to enter, except where one security area is within a larger, posted security area. The distance between the signage is to be determined by the CSA.

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 the Atomic Energy Act of 1954 and/or of the DOE Organization Act.
 - (c) A previous notice needs to be amended or revoked.
- (2) Contents.
 - (a) Each posting proposal must include 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 4c 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. Upon approval by the DOE Office of Health, Safety and Security, with concurrence by the Office of General Counsel, 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).
- (1) Property approved by the DOE Office of Health, Safety and Security should be posted at entrances and at such intervals along the perimeter of the property to ensure notification of persons about to enter. Signs should measure at least 11 x 14 inches (28 x 36 centimeters).
 - (2) The signs should be configured with a white or yellow background and black lettering. Signs that notify of the use of deadly force should use a white background with red lettering for the words "WARNING USE OF DEADLY FORCE AUTHORIZED." The remaining words should be in black.
 - (3) Placement of signs on fences must not interfere with the function of fence-mounted intrusion detection systems (IDS). If the signage interferes with the IDS or closed-circuit television coverage, it could be mounted on posts outside the fenced area. NOTE: The signage should be mounted so that it is easily discernable, midway between fence posts, at approximately 40-50 foot (12.1-15.1 meter) intervals.
- d. Notification to the Federal Bureau of Investigation. Notification, by the Office of Defense Nuclear Security, 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 Federal Bureau of Investigation exercising investigative responsibility over the property.

Chapter V - LOCKS AND KEYS

1. GENERAL REQUIREMENTS. A program to protect and manage locks and keys must be established by the cognizant security authority (CSA). The program must be applied in a graded manner based on the safeguards and security (S&S) interests being protected, identified threat, existing barriers, and other protection measures afforded these interests. 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. Alternate locking hardware may be used for the protection of Category I, II, III, and IV special nuclear material (SNM) and classified matter based on the vulnerability assessment. The CSA may approve alternate locking hardware at a lower level.
2. CATEGORIES. Security keys and locks are divided into three levels, Levels I through III. These levels are based on the S&S interest being protected and upon a site analysis. Non-security locks and keys are considered administrative. The CSA must determine the appropriate level for application to the site. Facilities that do not possess nuclear weapons, weapons components, SNM, classified matter, and high-value government property should follow the requirements established for Level III locks and keys. The paragraphs below describe recommended uses for each level.
 - a. Level I. Security locations such as vaults, closed areas, material access areas which store nuclear weapons and Category I and Category II that roll-up to a Category I quantity of SNM, and where Top Secret and/or Secret matter are stored require Level I security locks and keys. This applies to the innermost areas, not outer doors or gates.
 - b. Level II. Building doors, entry control points, gates in Protected Areas, fences, doors or other barriers or containers protecting Category II and Category III SNM and Confidential classified matter must be protected by locks and keys categorized as Level II.
 - c. Level III. Buildings, gates in fences, cargo containers, and storage areas protecting Category IV SNM, and government property whose loss would significantly impact security and/or site/facility operations must be protected by locks and keys categorized as Level III.
- NOTE: These requirements do not apply to the practice of “day-lock” for classified matter-in-use, a principle that is described in the NNSA *Information Security* NAP.
3. LOCK AND KEY STANDARDS. Key locksets must meet American National Standards Institute (ANSI) Standard A156.2-1996, *Grade 1, Bored and Preamsembled Locks and Latches*, or ANSI A156.13-1996, *Grade 1, Mortise Locksets*.

- a. Locks used in the protection of classified matter and Categories I and II SNM (e.g., security containers, safes, vaults) must meet Federal Specification FF-L-2740A, *Locks, Combination*.
- b. All security locks securing containers, vaults, and closed areas placed into service after July 14, 1994 must have a lock that meets Federal Specification FF-L-2740A, *Locks, Combination*.
- c. Combination padlocks must meet Federal Specification FF-P-110, *Padlock, Changeable Combination*, and standards cited in 41 *Code of Federal Regulations* (CFR) Part 101, Federal Property Management Regulations. These padlocks may be used with the lock bars securing metal filing cabinets. NOTE: These padlocks conform to the standards set forth in National Security Council Directive governing the classification, downgrading, declassification and safeguarding of national security information.
- d. Security key padlocks/hardware should meet the following specifications:
 - (1) High-security, shrouded-shackle, key-operated padlocks should meet standards in Military Specification MIL-DTL-43607H, *Padlock, Key Operated, High Security, Shrouded Shackle*. High-security padlocks are approved to secure Category I and II SNM and Top Secret and/or Secret matter.
 - (2) Low-security, regular (open-shackle, key-operated padlocks) should meet the classes and standards in Commercial Item Description A-A-59486A and A-A-59487A. The CSA must determine low-security padlock usage based upon the site analysis conducted on the security interest being protected.
 - (3) Lock bars used to secure file cabinets containing classified information must be 1¼ inches (31.75 millimeters) by 3/16 inch (4.76 millimeters) or equivalent in cross section and constructed of rigid metal material. NOTE: Securing file cabinets with locking bars will not be acceptable after October 1, 2012.
 - (4) Hasps and yokes on containers storing classified matter must be constructed of steel material, be at least ¼ inch (6.35 millimeters) in diameter or equivalent cross section, and be secured to the container by welding, or riveting, to preclude removal.
 - (5) General field service padlock is a heavy-duty, exposed shackle lock that meets Federal Specification FF-P-2827. The key-operated padlock is designed for non-high security application where there is exposure to grit and corrosive or freezing environments. The CSA must determine general field service padlock usage based on a site analysis conducted on the security interest being protected.

- e. 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 (see U.S. Department of Energy [DOE] M 470.4-7, *Safeguards and Security Program References*, dated 8-26-05).
 - f. Keys, key blanks, and key cutting codes must be protected in a graded fashion. Consideration must be given to the S&S interest being protected, the identified threat, existing barriers, and other protection measures afforded to the interest. Locks and keys must be categorized according to the interest being protected. An inventory and accountability system must be implemented.
 - g. Security key stock must be stored in a manner to prevent loss, theft, or unauthorized use. (Security keys are devices that can open a lock and can include, but are not limited to, 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 that may open a lock that controls access to a security interest must be protected from compromise. Personnel responsible for the control and issuance of locking systems and/or security keys, including key cards (when used in place of mechanical keys), must maintain a security clearance commensurate with that required for access to the interest to which the keys provide direct access.
 - (1) 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.
 - (2) The use and protection strategy for grand master, master, sub-master, and control keys, etc., must be considered, analyzed and documented in the Site Security Plan (SSP). Grand master and master keys will not be used in the protection of Category I SNM.
4. INVENTORY. 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 and documented in the SSP. A hands-on inventory must be conducted for all keys and padlocks both in use and in storage, as specified below. NOTE: The requirements for inventorying of locks do not apply to the XO series of combination locks installed on security containers, vaults and closed areas or electro-mechanical locks. Each accountable key and key core, including key cards (when used in place of mechanical keys), must have an affixed unique and permanent identifying number.
- a. Fabrication, issuance, return, and destruction of Levels I, II, and III security locks and keys must be documented.
 - (1) Duplicate and replacement keys must not have the same key number assigned as the key being replaced or duplicated.

- (2) Grand master security keys must be kept to an operational minimum and protected at the highest level of S&S interest being protected. NOTE: Grand master security keys include a system wherein a series of locks are keyed alike.
 - (3) The inventory record must identify the specific duplicate and replacement keys. If replaced, the disposition of the key being replaced must be recorded.
 - (4) Include in inventory records locks, keys in possession of key holders, issuance stock, and keys assigned to key rings/key cabinets. The inventory record should include the list of the locations of locks that each key will open.
 - (5) Document each person issued a Level I security lock and key and the individual who issued the locks and key.
 - (6) Document the locations of the locks and keys.
- b. There must be a 100 percent semi-annual inventory of all Level I security locks and keys.
 - c. Level I security keys issued on a temporary basis must be inventoried daily. Accountability of tamper indicating key rings is sufficient when used.
 - d. Key rings for Level I and II must have a unique identifying number placed on the ring.
 - e. A 100 percent inventory of all Level II keys must be conducted annually by the responsible organization. Level III keys will be inventoried as determined by the CSA.
 - f. Sites must have documented procedures for accountable key turn-in when personnel or programs are terminating or when an individual no longer has a need for the key.
5. LEVEL I SECURITY KEYS AND LOCKS. Level I key blanks must be restricted/proprietary; specifically, the blank must be unique to the site (e.g., it does not use a commercially available master key blank).
- a. When not in use for the protection of the above interests (e.g., locksmith service work) the 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 a General Services Administration (GSA)-approved security container or a closed area (or other location as identified in the SSP with equivalent protection). Access to the Level I security locks and keys must be controlled and limited to authorized personnel.

- b. Any installation, replacement, or maintenance activities associated with Level I security locks must be documented to include the name of a person who performed the activity.
 - c. The number of Level I keys must be kept to an operational minimum.
 - d. Level I keys must be on a separate key ring from all other levels of keys or as determined by the CSA.
 - e. 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 reported to the CSA as a lost/missing key as required.
 - f. Site-specific procedures must be developed for the control of Level I security lock and keys and be approved by the CSA.
 - g. Obsolete, damaged, or inoperative Level I keys must be destroyed in a manner that renders the key unusable and is authorized by the CSA and the destruction must be recorded.
 - h. In order for corrective actions to be taken quickly after an incident involving the loss, theft, or destruction of a Level I lock or key, a risk assessment and compensatory measures must be pre-established and documented.
 - i. When a Level I security key is unaccounted for, immediate notification must be made to the CSA, compensatory measures must be immediately initiated, and an incident of security concern inquiry must be completed. If the key cannot be located within 24 hours, the affected lock must be changed.
6. LEVEL II SECURITY KEYS AND LOCKS. When not in use for the protection of the above interests (e.g., locksmith service work) the assembled Level II security locks or cores and Level II security keys must remain under the direct control of an authorized person or must be stored in a GSA-approved security container or a closed area (or other location as identified in the SSP with equivalent protection). Access to the Level II security locks and keys must be controlled and limited to authorized personnel.
- 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 site without CSA approval.
 - 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 reported to the CSA as a lost/missing key.
 - d. Site-specific procedures must be developed for the control of Level II security lock and keys and be approved by the CSA.

- e. Obsolete, damaged, or inoperative Level II keys must be destroyed in a manner authorized by the CSA and such destruction recorded.
7. LEVEL III SECURITY KEYS AND LOCKS. All parts of broken Level III security keys should be recovered; if the functional part of the key (the blade) is lost or not retrievable, it must be reported to the CSA.
- a. Obsolete, damaged, or inoperative Level III keys must be destroyed in a manner authorized by the CSA and such destruction recorded.
 - b. Site-specific procedures must be developed for the control of Level III security locks and keys and be approved by the CSA.

Chapter VI - TESTING AND 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 implemented through locally developed planning documents and operational procedures. Testing and maintenance planning documents must include all security-related subsystems and components and must specify testing and maintenance frequencies.
2. LIFECYCLE PLANNING. Lifecycle planning must be conducted for major safeguards and security (S&S) equipment and component replacement, and must be documented in locally developed planning documents.
3. MAINTENANCE.
 - a. Corrective Maintenance. Corrective maintenance must be performed on security-related subsystems and components. A comprehensive maintenance prioritization plan must be established and approved by the cognizant security authority (CSA).
 - b. Compensatory Measures. Compensatory measures must be implemented immediately when any part of a critical system element protecting special nuclear material, classified matter, Sensitive Compartmented Information or Special Access Program interests is out of service. Compensatory measures must be approved by the CSA and must be continued until maintenance is complete and the system element is back in service.
 - c. Preventive Maintenance. Preventive maintenance must be performed on security-related subsystems and components in accordance with manufacturers' specifications and/or local procedures.

The following security-related subsystems and components must be included in a preventative maintenance program:

- (1) Intrusion detection and assessment systems and components, to include, tamper sensors, duress systems, and line supervision.
- (2) Long range detection and assessment systems.
- (3) Personnel and vehicle access control and entry/exit inspection equipment, to include package and hand-carried inspection equipment.
- (4) Systems utilized by the Protective Force for detection, assessment, or communication.
- (5) Security-related emergency power or auxiliary power supplies.
- (6) Security-related lighting.

- (7) Security barriers and delay mechanisms.
4. **TESTING.** An effective testing program provides both the reliability and assurance of security-related subsystems and components. Locally developed planning documents must identify testing frequencies for function and performance testing. Frequencies exceeding at least once every 12 months must be justified.
- a. The following security-related subsystems and components must be included in a testing program:
 - (1) Intrusion detection and assessment systems and components, to include, tamper sensors, duress systems, and line supervision.
 - (2) Long range detection and assessment systems.
 - (3) Radio frequency communications.
 - (4) Personnel and vehicle access control and entry/exit inspection equipment, to include package and hand-carried inspection equipment.
 - (5) Systems utilized by the protective force for the purpose of detection, assessment, and communication (to include those systems that provide communication capabilities to local law enforcement agencies).
 - (6) Security-related emergency power or auxiliary power supplies.
 - (7) Security-related lighting.

If testing indicates system degradation, it must be repaired and retested.

When calculating detection probability for multiple sensor systems, detection is assumed if any of the sensors report an intrusion as defined in the Site Security Plan.

Any time a system falls below the required probability of detection, the system must be repaired and retested.

- b. **Installation Test.** All newly installed systems must undergo an acceptance test. This test must be documented and includes both a function test and a performance test.
- c. **Function Test.** A function test is defined as – a test of a sensor or system that determines whether the minimum design requirements are being met (e.g., for an interior microwave intrusion detection sensor, a function test would confirm that the detection pattern and orientation are within design limits).
 - (1) A function test, in conformance with the manufacturer's specification, should be performed prior to acceptance of the installed system and thereafter as determined necessary by the CSA.

- (2) Testing must ensure that the alarm communication line or data link is capable of transmitting an alarm signal and that it has not been compromised.
 - (3) Alarm system components must be tested through physical actuation at a frequency documented in locally developed planning documents.
 - (4) Testing should be conducted to determine the proper settings for high detection rates with the lowest possible nuisance alarm rates.
- d. Performance Test. A performance test is defined as a test to ensure the ability of an implemented and operating system element, or total system, to meet established requirements.
- (1) The effectiveness of physical protection systems and programs must be determined through performance testing at a documented frequency in accordance with the Performance Assurance Program (see U.S. Department of Energy [DOE] M 470.4-1, Chg. 1, *Safeguards and Security Program Management*, dated 3-7-06).
 - (2) Testing Methodology – When planning and conducting performance testing, the following should be considered:
 - (a) Malevolent acts.
 - (b) Pathways to target from door or other engineered ~~moveable~~ opening unless specified by other site requirements.
 - (c) Adversary maneuvering and tactics (i.e., Tests should be consistent with Chapter X).
 - (3) If assessment is by closed circuit television, consider:
 - (a) Lowest lighting conditions that are routinely available.
 - (b) Worst case “light-to-dark ratio” to determine if shadows or dark spots in the field of view degrade assessment viability.
 - (c) Adverse weather and lighting conditions that are common to the local environment.
5. ESTABLISHED TESTING CRITERIA.
- a. Access Control Equipment. Screening equipment can include explosive detectors, metal detectors, and x-ray systems and must be capable of detecting

prohibited and controlled articles are detected before being permitted into DOE facilities

- (1) The following should be used as standard test weapons for metal detectors or the site must implement the performance testing procedures and test objects cited in Sections 5.1, 5.2 and the portion of 5.3 of National Institute of Justice Standard 0601.02, *Law Enforcement and Corrections Standards and Testing Program*, relating to non-ferromagnetic stainless steel knives:
 - (a) steel and aluminum alloy .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); or
 - (b) aluminum, model 7, .380 caliber Derringer manufactured by American Derringer Corporation (weight: about 200 grams); and
 - (c) stainless steel 0.22 caliber long rifle mini-revolver, manufactured by North American Arms (weight: about 129 grams).
- (2) X-ray machines may be used to 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 an unobstructed (discernable) set of wires and other objects as described in American Society for Testing and Materials (ASTM) standard for test objects (see ASTM Standard F792-01e2, *Standard Practice for Evaluating the Imaging Performance of Security X-Ray Systems*).
- b. Volumetric Devices. Tests for volumetric interior intrusion detection systems should consider a range of tests; i.e., walk tests, voltage variation, temperature and humidity, electromagnetic susceptibility, vibration, standby power, handling shock tests. Volumetric sensors must detect an individual walking at a rate of 1 foot per second within the total field of view of the sensor and its plane of detection. Testing beyond this design requirement must be approved in advance by the CSA for the purpose of sensitivity analysis.
- c. Backup Emergency Lighting. When back-up emergency lighting is used, it must be periodically tested to ensure that it will function as configured for a specified sustained period.
- d. Balanced Magnetic Switches (BMSs). 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 centimeters) from the door jamb or when the back edge clears the jamb.

6. TESTING AND MAINTENANCE PERSONNEL SECURITY CLEARANCES.
Personnel, who test, maintain, or service security-related subsystems components and system essential elements must have security clearances consistent with the S&S interest being protected, unless approved by the NNSA CSA.

7. RECORD KEEPING. Records of the failure and repair of security-related subsystems and components must be maintained as documented in local site procedures. Testing and maintenance records must be retained in accordance with the requirements of approved records management procedures.

Chapter VII - BARRIERS

1. GENERAL REQUIREMENTS. Physical barriers serve as the physical demarcation of the security area. Barriers such as fences, walls, turnstiles and doors must be used in Limited Areas (LAs) or above to deter and delay unauthorized access. At a minimum, an analysis is required of high-consequence security areas to determine the protection measures against Vehicle Borne Improvised Explosive Devices. Barriers may be used to support the prevention or mitigation of stand-off-attacks. Alternatives to the requirements specified in this chapter may be authorized as documented in the Site Security Plan (SSP).
 - a. Barriers must be used 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 and to provide the ability to identify and engage adversaries along all feasible pathways.
 - 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.
 - d. Barriers such as fences, walls, and doors may be used to identify the boundary of the property protection area and to provide protection. Barriers must be capable of controlling, impeding, or denying access to a security area.
 - e. Fences used should be installed no closer than 20 feet (6 meters) from the building or safeguards and security (S&S) interest being protected unless documented in the SSP and approved by the cognizant security authority (CSA).
 - f. These requirements must be consistent with the operation of the facility and protection goals as documented in the vulnerability assessment.
2. PENETRATION OF SECURITY AREA BARRIERS. Penetration of security area barrier requirements includes the following:
 - a. 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 being penetrated.
 - b. Utility corridors that penetrate security area barriers must provide the same degree of penetration resistance as the barriers they penetrate.
 - c. Objects that intruders could use to scale or bridge barriers and enter security areas must be removed or secured to prevent their unauthorized use.
 - d. If a security area configuration is altered, (e.g., during construction or temporary activities), equivalent protection measures must be implemented and documented.

- e. The barrier design must consider proximity to buildings or overhanging structures.
3. HARDWARE. Screws, nuts, bolts, hasps, clamps, bars, wire mesh, hinges, and hinge pins must be fastened securely to impede 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) or by other means as described in the SSP. NOTE: These requirements do not apply to fencing.
 4. FENCING. When used to protect security areas designated as Protected Areas (PAs) or higher, fencing must meet the following requirements.
 - a. PA or Higher Fencing Materials and Specifications.
 - (1) Chain link fabric consisting of a minimum of No. 11 American Wire Gauge (AWG) or heavier galvanized steel wire with mesh openings not larger than 2 inches (5.08 centimeters) on a side must be used at security areas. This fencing must be topped by three or more strands of barbed wire single or double outriggers. Double outriggers may be topped with coiled barbed wire (or with a barbed tape coil). The direction of the outrigger is at the discretion of the CSA.
 - (2) Overall fence height, excluding barbed wire or barbed tape coil topping, must be a minimum of 7 feet (2.13 meters).
 - (3) Fence lines must be kept clear of vegetation, trash, equipment, and other objects that could impede observation or facilitate bridging.
 - (4) Gate hardware that if removed would facilitate unauthorized entry must be installed in a manner to mitigate tampering and/or removal (e.g., by brazing, peening, or welding).
 - (5) Posts, bracing, and other structural members must be located on the inside of security fences.
 - b. Limited Area (LA) Fencing Materials and Specification. When used to protect security areas designated as LAs, fencing must meet the following requirements.
 - (1) Barriers such as fences, walls, and doors may be used to identify the boundary of the LA and to provide protection and security area demarcation. Barriers must be capable of controlling and impeding access to a LA.
 - (2) Overall fence height, excluding barbed wire or barbed tape coil topping, must be a minimum of 6 feet.

- evidence of penetration of the security area or access to the security interest being protected.
7. CEILING AND FLOORS. Ceilings and floors must be constructed of building materials that offer penetration resistance to, and evidence of, unauthorized entry into the area.
 8. DOORS. Doors, door frames, and door jambs associated with walls serving as barriers must provide the necessary barrier delay required by the SSP. Requirements include the following.
 - a. Penetration Resistance Doors. Doors with transparent glazing material must offer penetration resistance to, and evidence of, unauthorized entry into the area. Doors that serve exclusively as emergency and evacuation exits from security areas must not be accessible from outside the security area.
 - b. Astragals or Mullions. An astragal or mullion must be used where doors used in pairs meet. Door louvers, baffles, or astragals/mullions must be reinforced and immovable from outside the area being protected.
 - c. Visual Access. A sight baffle must be used if visual access is a factor.
 9. 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.
 10. PROTECTIVE FORCE (PF) POSTS.
 - a. Special Nuclear Material (SNM) Access. Permanent PF posts controlling access to protected areas and PF towers intended to be used as a tactical fighting position should be constructed to meet the requirements for a hardened post, unless documented through vulnerability analysis in the SSP or documented in the SSP. Exterior walls, windows, roofs, floors (towers only) 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 Underwriters Laboratories (UL) Standard 752, *Standard for Bullet Resisting Equipment*.
 - b. Fighting Positions. Designated fighting positions must be sited in locations that command significant fields of fire and must be able to serve as bases of maneuver for PF tactical units. These positions must afford protection as documented through vulnerability assessments in the SSP.

11. UTILITY AND OTHER BARRIER PENETRATIONS AND OPENINGS. The following requirements apply to security areas other than GAAs, Property Protection Areas (PPAs) and LAs. The application to GAAs, PPAs and LAs is at the discretion of the CSA.

Physical protection features must be implemented at all locations where utility and other barrier penetrations and openings occur, such as where storm sewers, drainage swales, and site utilities intersect the security boundary or area. These openings/penetrations must be sealed/filled or constricted barriers applied to deter and/or prevent an unauthorized entry. In those instances where a potential audio/video surveillance threat could occur within conference rooms and other similar facilities approved for classified discussions the provisions of the NNSA *Information Security* NAP should be implemented. Barriers or alarms are required for all miscellaneous openings for which:

- a. 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;
- b. 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; the opening is not visible from another controlled opening in the same barrier; or the opening is below a perimeter barrier, which is part of a utility tunnel, pipe chase, exhaust ducts or air handling filter banks penetrating the building, facility, or site.

12. PENETRATION OF PA/MATERIAL ACCESS AREAS (MAA) BARRIERS. In addition to the requirements in Section 11 above, penetration of security area barrier requirements for a PA includes the following:

- a. Overhead utilities must not allow for access into a PA or higher security area without physical protection features to deter or detect unauthorized access into the security area.
- b. Two permanent, continuous parallel fences (requirement for the perimeter intrusion detection and assessment system) must identify the boundary of the PA.
- c. Barrier requirements for a material access area include those required for a PA in addition to the following:
 - (1) 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.

- (2) Doors at entry control points such as transfer locations must be alarmed, and the alarms must communicate with the central alarm station/ secondary alarm station when an unauthorized exit occurs.
 - (3) 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. Exits designed for emergency evacuation must be alarmed with an intrusion detection system or controlled at all times.
13. BARRIERS-DELAY MECHANISMS. Mechanisms must be used to deter and delay access, removal, or unauthorized use of Category I and II quantities of SNM and nuclear weapons.
 - a. Delay mechanisms may include both passive physical barriers (e.g., walls, ceilings, floors, windows, doors, and security bars) and activated barriers (e.g., sticky foam, pop-up barriers, cold smoke, and high-intensity sound). The appropriate delay mechanisms must be used at site-specified target locations to reduce reliance on PF recapture/recovery operations.
 - b. Active and passive denial systems should be considered, as appropriate, to reduce reliance on recapture operations.
14. ACTIVATED BARRIERS, DETERRENTS, AND OBSCURANTS. If used, activated barrier and deterrent systems must meet site-specific requirements when deployed at improvised nuclear device/radiological dispersal device denial target locations. Activated barriers, deterrents, and obscurants must meet the following requirements:
 - a. Obscurants must consider spatial density versus time to deploy as determined by vulnerability analysis.
 - b. Dispensable materials must be individually evaluated for effectiveness of delay.
 - c. Controls and dispensers must be protected from tampering and must not be co-located.
15. VEHICLE BARRIERS. Vehicle barriers must be used to deter and impede penetration into security areas when such access cannot otherwise be controlled.
 - a. At Category I/II facilities, all potential vehicle approach routes to identified target areas must have barriers installed that will impede an adversary and achieve site-specific threat/target system response requirements.
 - b. Controls for motorized gates/vehicle barriers used for entry control points must be located within PF posts or other protected locations as described in the SSP. Motorized gates must be designed to facilitate manual operation during power outages.

Chapter VIII - COMMUNICATIONS, ELECTRICAL POWER AND LIGHTING

1. COMMUNICATIONS. Communications equipment must be provided to facilitate reliable information exchanges between protective force personnel. Security system transmission lines and data must be protected in a graded manner from tampering and substitution. Communications equipment for facilities protecting Category I and II quantities of special nuclear material (SNM) must meet the following requirements.
 - a. Redundant Voice Communications. Facilities protecting Category I and II quantities of SNM must have a minimum of two different voice communications technologies to link the central alarm station (CAS)/secondary alarm station (SAS) to each fixed post and protective force (PF) duty location. Alternative communications capabilities must be available immediately if the primary communications system fails. Radio systems used for critical protective force communications must have the ability to prioritize radio traffic to ensure the highest availability to PF communications.
 - b. Recording of Communication. A continuous electronic recording system must be provided for all security radio traffic and telecommunications that provide support to the CAS. The recorder must be equipped with a time track and must cover all security channels. Sites must follow the established requirements for consensual listening-in to or recording telephone/radio conversations as contained in U.S. Department of Energy (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.
 - d. Communication Systems. Protection system communications must support PF communications. PF communications include the hardware that enable officers to communicate with each other.
 - (1) Design Considerations. The design of a PF communication system must address resistance to eavesdropping, vulnerability to transmission of deceptive messages, and susceptibility to jamming.
 - (2) PF Radio System Requirements. The application of digital encryption may be implemented on a graded basis. When the PF communications are converted to meet Federal Communications Commission narrow band frequency requirements, digital encryption (see ANSI/TIA/EIA-102 Phase I, referred to as Project 25) must be included.
 - (3) 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. Encryption is not required for alternate means of communication.

- (4) Local Law Enforcement Agency (LLEA) Communication. If required by the Site Security Plan (SSP), a mechanism must be established to ensure communication with LLEAs. An alternative communications capability from a SAS must be provided if the primary station is compromised. Tests of these communications systems must be documented in the local site procedures and the memorandum of agreement/understanding.
- e. Duress Systems. Facilities with protected areas and material access areas must have duress notification capabilities for mobile and fixed posts and for the CAS/SAS. The duress system must meet the following requirements.
- (1) 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.
 - (2) The duress alarm for a CAS must annunciate at the SAS while the duress alarm for the SAS must annunciate at the CAS.
 - (3) Mobile duress alarms must annunciate at the CAS, SAS, or another fixed post.
 - (4) All PF fixed posts must have duress devices (see DOE M 470.4-3A, *Contractor Protective Force*, dated 11-5-08).
- f. Radios. Fixed-post radios, mobile radios, and portable radios must be provided to support operational security requirements.
- (1) Radio System Requirements.
 - (a) The radio system must be capable of accessing security operations.
 - (b) Radios must have power and sensitivity for two-way voice communications with the facility base stations.
 - (c) Security communication must be restricted to security operations.
 - (d) Radio system components must be protected against unauthorized access.
 - (2) Portable Radios. Portable radios must be capable of two-way communication on the primary security system. An alternative means of communications must be provided if safety, process procedures, or facility structure prohibit transmission within a building or structure.

- (3) Two-Way Communications. Radios must be capable of maintaining two-way communication with the CAS/SAS.
 - (4) Emergency Response Communications. Base stations, which are controlled from the CAS, must be capable of communicating with emergency response systems/personnel.
 - (5) 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.
 - (6) Repeater Stations. A radio repeater station must be placed in a location that ensures all-weather access for vehicles and personnel to the station building, antenna, standby generator plant, and fuel storage tanks. The station must be designed to minimize risk of damage to the antenna structure and supporting guy lines from vehicular traffic.
- g. PF Tracking Systems. Systems capable of tracking and displaying the live movements and state-of-health of PF may be used to improve the situational awareness of PF commanders. Data associated with these systems are typically transmitted by radio frequency so the following limitations apply:
- (1) Classified information may not be transmitted by the wireless communications associated with tracking systems.
 - (2) PF tracking systems used at sites with Category I quantities of SNM must be evaluated prior to implementation by the CSA. The evaluation is to determine if the high system effectiveness rating, as described in DOE M 470.4-1, Chg. 1, *Safeguards and Security Program Management*, dated 3-7-06 would be degraded if compromised unless encrypted.
- h. Radio Frequency (RF) Alarm Communications. The RF alarm communications systems, when used to protect Category I and II quantities of SNM, must be limited to emergency, temporary situations, or early warning detection applications. When used, a comprehensive risk assessment must be conducted and a DOE O 470.3B, *Graded Security Protection (GSP) Policy*, dated 8-12-08, implementation plan established. RF alarm systems and associated communication systems used for the protection of Category I and II quantities of SNM must meet the following additional requirements:
- (1) RF alarm communications systems are used for auxiliary security applications and do not require the same robustness as primary systems for protection of Category I and II quantities of SNM.
 - (2) Use of a RF alarm communications system must be evaluated prior to implementation by the CSA and determined to not affect a high system

effectiveness rating as described in DOE M 470.4-1, Chg. 1, if compromised.

2. ELECTRICAL POWER. Power supply elements located or operating within the confines of the site should be protected from malicious physical attacks based on a documented local site determination of impact. The site must determine the need for auxiliary power based on safeguards and security interests being protected and document it in the SSP.

Electrical power to supply the intrusion detection and assessment systems should be provided to assure continuous system availability and operation. The scope of the primary and auxiliary power sources are as follows.

- a. Primary Power. All intrusion detection systems (IDSs) must have primary power from normal onsite power. The power source must contain a switching capability for component and comprehensive system testing. This testing can be used to determine the capacity and source of the required auxiliary power. Early warning systems and other technologies that have self-contained electrical power are exempt from this requirement. The following system elements should be considered in configuring the power requirements:
 - (1) Alarm data networks and communication systems should receive primary power directly from the onsite power distribution system. When the facility does not receive its power from an internal distribution system, power would come directly from the public utility.
 - (2) Alarm control panels, alarm management systems and automated information systems or associated critical components must be connected to an uninterruptible power supply or auxiliary power.
 - b. Auxiliary-Uninterruptible Power. Auxiliary or uninterruptible power sources should be provided for alarm systems requiring continuous power and for systems that, if interrupted, would degrade or compromise the protection afforded the asset.
3. ELECTRICAL POWER FOR CATEGORY I AND II FACILITIES. All IDSs protecting safeguards and security interests must have a primary power source from normal onsite power. Early warning systems and other technologies that have self-contained electrical power are exempt from this requirement. Power sources must contain a switching capability for operational testing to determine required auxiliary power sources. The following power supply requirements apply:
 - a. 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.

- b. 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.
 - c. Radio System 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.
 - d. Auxiliary Power Sources. Intrusion detection and assessment, automated access control, and closed circuit television (CCTV) systems protecting Category I and II quantities of SNM must have an auxiliary power capability.
 - (1) Transfer to auxiliary power must be automatic upon failure of the primary source and must not affect operation of the protection system, subcomponents, or devices. The CAS and SAS must receive an alarm indicating failure of the protection system's primary power.
 - (2) When used, rechargeable batteries 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 based on manufacturer's recommendations. The system must be capable of generating a low-battery alarm that shall be transmitted to the CAS and SAS unless the system is also on a UPS.
 - (3) Power sources must be tested in accordance with site procedures.
 - e. Uninterruptible Power Supply. 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 to an unacceptable level.
4. LIGHTING. Lighting systems are deployed for detection and assessment of unauthorized persons. Protective system lighting, as defined in the SSP, should be applied consistent with the following principles:
- a. 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;
 - b. 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;
 - c. ensure that compensatory measures are implemented when the lighting system fails;
 - d. be maintained and tested in accordance with locally approved procedures;

- e. when possible not illuminate patrol paths other than at entry control points;
 - f. when applicable illuminate the area outside the fence line or barrier so that it will expose anyone approaching the coverage area and limit the vision of anyone outside of the fence or barrier;
 - g. complement the electro-optical/CCTV assessment systems;
 - h. illuminate the area within the fence/barrier boundary or the exterior of a building;
 - i. be configured to impede open access to the lighting controls; and
 - j. allow for the rapid and reliable assessment of alarms from either the CCTV system or response personnel.
5. LIGHTING FOR CATEGORY I AND II FACILITIES. Lights must support a 24-hour visual assessment and provide, as a minimum, 2 foot-candle illumination at ground level for at least a 30-foot (9.14-meters) diameter around PF posts and a minimum of 0.2-foot candle illumination within the Perimeter Intrusion Detection and Assessment System (PIDAS) isolation zone.
- a. Sufficient lighting for assessment must be maintained on the PIDAS sensor zones and the clear zones for CCTV assessment and surveillance 24 hours a day. The lighting must compliment the CCTV system in supporting its video assessment capability.
 - b. Where protective lighting at remote locations is not feasible, PF patrols and/or fixed posts must be equipped with night-vision and/or thermal imaging devices. Night-vision and/or thermal imaging devices should not be used routinely in lieu of protective lighting at entrances and exits but may be used if lighting is lost.
 - c. Light glare must be minimized whenever possible.
 - d. Light sources on protected perimeters must be located so that illumination is directed outward so that the PF is not blinded or silhouetted.
 - e. When back-up emergency lighting is used, it must be periodically tested to ensure that it will function as configured for a specified sustained period.

Chapter IX - SECURE STORAGE

1. GENERAL REQUIREMENTS.

- a. Secure Storage. The storage requirements for classified matter can be found in the NNSA *Information Security* NAP.
- b. Access Controls. Access to vaults and closed areas (CAs) must be strictly controlled and based on an appropriate security clearance and need-to-know.
 - (1) Need-to-know includes incidental access, i.e., access granted to individuals who handle or come into contact with classified matter but whose job functions do not include review or other use of the classified matter.
 - (2) Means of controlling access must be documented in a Site Security Plan (SSP).
- c. Miscellaneous Openings. All vents, ducts and similar openings into CAs that measure in excess of 96 square inches (619.20 square centimeters) and over 6 inches (15.24 centimeters) in their 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 must be protected with either ½-inch diameter steel bars with a maximum space of 6 inches between the bars; grills consisting of 18-gauge expanded metal, wire mesh; or an equivalent gauge metal duct barrier; or alternative measures as approved by the cognizant security authority (CSA). The barriers must be secured to preclude removal from outside the area, and the method of installation must ensure that classified matter cannot be removed through the openings with the aid of any type of instrument. A barrier will not be required if an approved intrusion detection system (IDS) provides protection of the opening.

2. VAULTS AND CLOSED AREAS. The standards required for construction of vaults and CAs, other than General Services Administration (GSA)-approved modular vaults, apply to all new construction, reconstruction, alterations, modifications and repairs.

Vault construction standards must comply with Federal Standard 832, *Construction Methods and Materials for Vaults*.

CA construction standards must comply with the requirements of this NNSA Policy. The CSA must approve all construction types and the methods used before the storage of classified matter or safeguards and security (S&S) interests is authorized.

- a. Vaults. A vault must be a penetration-resistant, windowless enclosure that has doors, walls, floor, and roof/ceiling designed and constructed to significantly delay penetration from forced entry and equipped with IDS devices on openings allowing access. The material thickness must be determined by the requirement for forcible entry delay times for the S&S interests stored within but must not be

less than the delay time provided by a minimum 8-inch (20.3 2-centimeters)-thick reinforced concrete poured in place, with a minimum 28-day compressive strength of 2,500 pounds per square inch (17,237 kilopascal). Technologies such as activated barriers or passive/active denial systems may be used in lieu of thicker concrete when analysis indicates that delay times exceeding that of 8-inch (20.3 2-centimeters)-thick reinforced concrete are required. The site's analysis of protection measures used must be documented in its SSP. For new vault construction, Federal Standard 832, *Federal Standard Construction Methods and Materials for Vaults* must be used.

- (1) Vault Door. A vault door and frame must meet the GSA's highest level of penetration resistance. The lock on the door must be a minimum of a GSA-approved lock.
 - (2) Wall Penetrations. Any miscellaneous openings of a size and shape to permit unauthorized entry (larger than 96 square inches [619.2 square centimeters] in area and more than 6 inches [15.24 centimeters] in its smallest dimension) must be equipped with barriers such as wire mesh, 9-gauge expanded metal or rigid steel bars at least 0.5 inches (1.3 centimeters) in diameter secured in a way to prevent unauthorized removal; e.g., 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 used, wire mesh, expanded metal, or rigid steel bars must be mounted so that special nuclear material (SNM) cannot be removed. The annular space between the sleeve and the pipe or conduit must be filled to show evidence of surreptitious removal.
 - (3) 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 with locks and intrusion detection alarms as specified in paragraph 4 of this Chapter.
- b. Closed Areas. Due to the size and nature of the classified matter, or for operational necessity, it may be necessary to construct CAs for storage because GSA-approved containers or vaults are unsuitable or impractical. Access to CAs must be controlled to preclude unauthorized access. This may be accomplished through the use of a cleared person or by a supplanting access control device or system. Access shall be limited to authorized persons who have an appropriate security clearance and a need-to-know for the classified matter/information within the area. Persons without the appropriate level of clearance and/or need-to-know shall be escorted at all times by an authorized person where inadvertent or unauthorized exposure to classified information cannot otherwise be effectively prevented. CAs storing TOP SECRET and SECRET matter shall be accorded supplemental protection during non-working hours. During non-working hours and during working hours when the area is unattended, admittance to the area shall be controlled by locked entrances and exits secured by either an approved

built-in combination lock or an approved combination or key-operated padlock. Alternate locks for a CA protecting classified matter inside a PA may be approved by the CSA. It is not necessary to activate the supplemental controls during working hours. Doors secured from the inside with a panic bolt (for example, actuated by a panic bar, a dead bolt, a rigid wood or metal bar) or other means approved by the CSA, will not require additional locking devices.

- (1) Procedures will be developed and implemented to ensure the structural integrity of CAs above false ceilings and below raised floors.
- (2) Open shelf or bin storage of SECRET and CONFIDENTIAL documents in CAs requires CSA approval. For SECRET matter only areas protected by an approved IDS will qualify for such approval. Open shelf or bin storage of TOP SECRET documents is not permitted.
- (3) The CSA may grant self-approval authority to the Facility Security Officer (FSO) for CA approvals provided the FSO meets specified qualification criteria as determined by the CSA.
 - (a) Hardware. Only heavy-gauge hardware shall be used in construction. Hardware accessible from outside the area shall be peened, pinned, brazed or spot welded to preclude removal.
 - (b) Floors and Walls. Construction may be of material offering resistance to, evidence of, unauthorized entry into the area. If insert-type panels are used, a method shall be devised to prevent the removal of such panels without leaving visual evidence of tampering. If visual access is a factor, area barrier walls shall be of opaque or translucent construction.
 - (c) Windows. Windows that can be opened and that are less than 18 feet from an access point (for example, another window outside the area, roof, ledge, or door) shall be fitted with ½-inch bars (separated by no more than 6 inches), plus crossbars to prevent spreading, 18-gauge expanded metal or wire mesh securely fastened area on the inside and made non-removable if mounted on the exterior of the CA. When visual access of classified information is a factor, the windows shall be covered by any practical method, such as drapes, blinds, or paint covering the inside of the glass. During nonworking hours, the windows shall be closed and securely fastened to impede surreptitious entry.
 - (d) Doors. Doors shall be constructed of material offering resistance to and detection of unauthorized entry. When windows, louvers, baffle plates, or similar openings are used, they shall be secured with 18-gauge expanded metal or with wire mesh securely fastened

on the inside and made non-removable if mounted on the exterior of the CA. If visual access is a factor, the windows shall be covered. When doors are used in pairs, an astragal (overlapping molding) shall be installed where the doors meet.

- (e) Ceilings. Ceilings shall be constructed of material offering resistance to and detection of unauthorized entry. Wire mesh or other non-opaque material offering similar resistance to, and evidence of, unauthorized entry into the area may be used if visual access to classified matter is not a factor.
 - (f) Ceilings (Unusual Cases). When wall barriers do not extend to the true ceiling and a false ceiling is created, the false ceiling must be reinforced with wire mesh or 18-gauge expanded metal to serve as the true ceiling or ceiling tiles must be secured. When wire mesh or expanded metal is used, it must overlap the adjoining walls and be secured in a manner that precludes removal without leaving evidence of tampering. When wall barriers of an area do extend to the true ceiling and a false ceiling is added, there is no necessity for reinforcing the false ceiling. When there is a valid justification for not erecting a solid ceiling as part of the area, such as the use of overhead cranes for the movement of bulky equipment within the area, the contractor shall ensure that surreptitious entry cannot be obtained by entering the area over the top of the barrier walls.
3. CA ROOM COMPLEX. CA S&S criteria may be extended to multiple rooms including an entire building. CA room complexes must meet the standards and construction requirements identified in paragraph 2 above.
- a. Interior walls may extend to a false ceiling and/or raised floor. Interior doors, windows, and openings may exist between different work areas. 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 or other systems as approved by the CSA.
 - b. Protective measures must be consistent with requirements for CA IDS (paragraph 4. below), but implemented at the building level.
4. IDS. IDSs are required for vaults and CAs and in some instances where certain types of containers are used to store S&S interests. For CAs and vaults protecting SECRET matter in a PA, the PIDAS meets the requirement for an IDS. The IDS must be placed in secure mode at the end of daily operations.
- 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 engineered opening to allow detection of attempted or actual unauthorized access.

- b. CAs protecting SNM must be able to provide effective protection against credible malevolent attacks and other hostile actions. Appropriate controls will be implemented based on site needs as identified in the GSP.
 - c. CAs Protecting Classified Matter and when used for Category III and IV SNM. A BMS or equivalent device and volumetric or equivalent coverage must be used on each door or engineered opening to allow detection of attempted or actual unauthorized access. A CA within a PA does not require an IDS.
 - d. CAs Protecting Category I and II SNM. A BMS or equivalent device must be used on each door or engineered opening. The security interest must be surrounded by an IDS or the IDS must be able to detect penetration of the entire surrounding perimeter such that physical access is detected via any credible pathway as approved by the CSA. If the CA is within a Material Access Area (MAA), detection coverage for the CA may be provided by IDS both inside the CA and/or outside the CA but within the MAA.
5. SECURITY CONTAINERS. The GSA establishes the national standards and specifications for commercially manufactured security containers or cabinets. Containers purchased after July 14, 1994, must conform to the latest GSA standards and specifications. Steel filing cabinets with rigid metal lock bar and approved three position, dial-type, changeable combination locks, purchased and approved for storage of SECRET matter may continue to be used until October 1, 2012. If steel filing cabinets are used to store classified matter, the supplemental controls specified in the *NNSA Information Security NAP* must be implemented.
- a. Requirements.
 - (1) Label and Mark. A security container must bear a test certification label on the inside of the locking drawer or door and must be marked “GSA-Approved Security Container” on the outside of the top drawer or door.
 - (2) Maintenance. A history for each security container describing damage sustained and repairs accomplished must be recorded on Optional Form 89, *Maintenance Record for Security Containers/Vault Doors* and retained for the life of the security container.
 - b. Damage and Repair of GSA-Approved Security Containers. Neutralizing lock-outs or repairing any damage that affects the integrity of a security container approved for the storage of classified matter must be conducted by cleared or escorted safe technicians or locksmiths.
 - (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 approved by GSA.
- 6. NON-CONFORMING STORAGE. Non-conforming storage is a means of providing equivalent storage protection for classified matter that cannot be protected by established standards and requirements due to size, nature, operational necessity, or other factors. Authority and protection requirements for non-conforming storage are provided in the NNSA *Information Security* NAP.

Chapter X - INTRUSION DETECTION AND ASSESSMENT SYSTEMS

1. GENERAL REQUIREMENTS. Where applicable, intrusion detection and assessment systems may be used to protect classified matter and Category III or higher special nuclear material (SNM) and other safeguards and security (S&S) interests as identified in the Site Security Plan (SSP). Intrusion detection systems (IDS) are required for vaults, closed areas (CAs), and, in some instances where certain types of containers are used. For CAs and vaults protecting Secret matter in a Protected Area (PA), the Perimeter Intrusion Detection and Assessment System (PIDAS) meets the requirement for an IDS. IDS must protect the security interests as defined in Chapter IX.
 - a. IDSs must perform in all environmental conditions and under all types of lighting conditions as defined in the SSP, otherwise compensatory measures must be implemented.
 - b. An effective method must be established for assessing all IDS alarms to determine the cause in a timely manner.
 - c. Closed circuit television assessment cameras used as primary assessment for alarms should be fixed (i.e., not pan or tilt) with fixed focal length lenses or may have a zoom capability.
 - d. Response capability to IDS alarms must be provided by assigned protective force (PF) personnel, by local law enforcement agency, or other authorized personnel as documented in the SSP.
 - e. For performance testing requirements, see Chapter VI.
 - f. The false and nuisance alarm threshold rates are determined after analysis and evaluation. The cognizant security authority (CSA) develops written false alarm rates/nuisance alarm rates parameters based on the analysis and site-specific conditions, seeking to achieve "As Low As Reasonably Achievable" levels. Absent a documented risk analysis the following minimum requirements must be applied:
 - (1) Each interior intrusion detection sensor should not have a false or nuisance alarm rate of more than one alarm per 2400 hours of operation while maintaining proper detection sensitivity.
 - (2) Each exterior intrusion detection sensor should not have a false or nuisance alarm rate of more than one alarm per 24 hours of operation while maintaining proper detection sensitivity.
 - (3) Interior IDS used to protect munitions/explosives storage igloos/bunkers should not have false or nuisance alarm rates exceeding one alarm per 400 hours of operation while maintaining proper detection sensitivity.

- g. The IDS must be designed, installed, operated, and maintained to ensure that the number of false and nuisance alarm do not reduce confidence level.
 - h. Each alarm occurrence, regardless of the cause, must be documented for analysis and trending purposes.
 - i. The IDS must be designed, where economically feasible, with independent redundant data communication paths for protecting S&S interests. The paths must be documented in an SSP or protection procedures, consistent with Table 1, Line Supervision Protection.
2. INTERIOR IDS REQUIREMENTS. The following requirements apply to interior IDS:
- a. Interior Systems. Interior systems must be designed, installed, and maintained to detect adversaries.
 - b. Balanced Magnetic Switches (BMSs). 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 centimeters) from the door jamb or when the back edge clears the jamb.
 - c. Volumetric Devices. Volumetric sensors must detect an individual walking at a rate of 1 foot per second within the total field of view of the sensor and its plane of detection.
3. EXTERIOR IDS REQUIREMENTS. The IDS 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 consistent with vulnerability assessments .
- When calculating detection probability for multiple sensor technology systems, detection is assumed if any of the sensors/zones report an intrusion.
4. RADIO FREQUENCY ALARM COMMUNICATIONS. Radio frequency alarm communications are appropriate when used for the protection of government property and classified matter. An IDS may use radio frequency communications to transmit alarm and other data for alarms, video, and other data utilized by the IDS provided:
- a. The data being transmitted are not classified.
 - b. The data being transmitted are protected consistent with the program office cyber security plan and DOE requirements (see DOE M 205.1-3, *Telecommunications Security Manual*, dated 4-17-06).
5. PROTECTION OF IDS.
- a. General Requirements. System components protecting sensitive compartmentalized information facilities, special access program facility, SNM

and classified matter activities must be protected with tamper indication in both the access and the secure modes. Tamper indication is required for intrusion detection/alarm devices. Tamper switch wiring must be as listed below.

- (1) Communication links, data gathering panel/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 Underwriters Laboratories (UL) Standard 681, *Standard for Installation and Classification of Burglar and Holdup Alarm Systems*.
 - (2) All tamper switches (e.g., sensors, processors, cable terminal boxes, control units, etc.) 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.
 - (3) The switches may be wired as part of the line supervision circuit per UL Standard 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.
 - (4) Commercial central alarm station service firms must issue a current UL certification commensurate with the contracted service and must maintain this UL certification as long as the service is provided to the facility. For the protection of classified matter UL Standard 2050, *National Industrial Security Systems for the Protection of Classified Materials*, should be implemented and a certificate issued for compliance with the UL standard. For other non-classified matter applications, UL Standard 1076, *Proprietary Burglar-Alarm Units and Systems*, should be implemented and a certificate issued for compliance with the UL standard.
- b. Enclosures and Junction Boxes. Permanent junction boxes, field distribution boxes, cable terminal boxes, and cabinets (equipment that terminates, splices, and groups interior or exterior IDS input or that could allow tampering, spoofing, bypassing, or other system sabotage) must be afforded tamper protection or tamper-resistant hardware. Tamper switches must provide a tamper indication to the annunciators. Manholes and other enclosures, if serving as a junction box for data communication cables, must be protected from unauthorized access.
- c. Line Supervision. Line supervision is required for IDSs protecting S&S interests. For property protection areas, line supervision may be provided consistent with a documented cost/benefit analysis as determined by the CSA. 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 in Table 1, Line Supervision Protection. In the event line security is not

available, the equipment that is utilized to transmit and receive signals between the protected area and the monitoring location shall comply with either UL Standard 1076 or UL Standard 1610.

- (1) Line Supervision Options. Different combinations of line supervision are allowed depending on link routing:
 - (a) An alarm communication link remaining within the security area and alarm communication link going through a lower security area.
 - (b) Line supervision is required for the two primary segments of alarm data transmission: from sensor to data gathering panel (DGP)/field processor and from DGP/field processor to DGP/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, digital communications (UL Classes A through C), apply to alarm communication links between DGPs/field processors, between DGPs/field processors and central alarm computers or alarm annunciator panels, and between computers.
 1. For Class A, the data transmission must comply with DOE requirements (see DOE M 205.1-3, *Telecommunications Security Manual*, dated 4-17-06).
 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, non-encryption over fiber optic cable enclosed in conduit, or
 - c 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) In general, analog signals (UL 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 alternating current (AC), be pulsed direct current (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 outside of a vault or CA must be as listed below.
 - (a) Protection for communication links must meet the supervised circuit requirements for the National Electric Code for protection from damage (see UL Standard 681).
 - (b) Wiring must be protected from access under the following conditions:
 - 1. for runs between the sensor and the field processor, when the wiring is under Class F line supervision;
 - 2. wiring protecting Top Secret;
 - 3. when the DGP/field processor is outside of the area being protected.
 - (c) Acceptable methods for protecting alarm system wiring are as follows:
 - 1. a totally concealed or embedded conduit system;
 - 2. junction boxes, pull boxes and other openings sealed by welding, epoxy-sealed threads, locked cover plates, tamper-resistant screws, or tamper alarm switches;
 - 3. alarm coverage of all wiring; or,
 - 4. armored cable/wire, compression coupled, electro-mechanical tubing or threaded conduit.
- d. Alarm Annunciation.
 - (1) Line supervision alarms Classes A through C must annunciate in central alarm station (CAS)/secondary alarm station (SAS) indicating the type of

- alarm (data error, loss of communication, tamper, etc.) and the affected equipment.
- (2) Sensor to DGP/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.
 - (6) Compensatory measures must be implemented to protect the alarmed location until required testing and repairs are completed.

Table 1. Line Supervision Protection

Communication Lines between a Field Processor and Field Processor or a Central Processor			
	CAT I or II SNM, Top Secret Classified Matter	CAT III or IV SNM, Classified Matter Secret and below	Maximum Internal System communications Supervision interval
	Class of Supervision	Class of Supervision	(ALL)
Routed within the alarm area	C	C	15 minutes
Routed through a lower security area	B	C	10 minutes
Routed through an unsecured area	A	B	5 minutes
Wiring from the sensor to the DGP			
All field wiring	F	F	Continuously

6. GENERAL REQUIREMENTS FOR CATEGORY I AND II QUANTITIES OF SNM. Nuclear weapons and Category I and II quantities of SNM must be protected by an integrated physical protection system using protective force, barriers, and Intrusion Detection and Assessment Systems (IDAS).
 - a. Protecting SNM. The following requirements apply for alarms protecting Category I and II quantities of SNM.
 - (1) Interior or exterior IDASs must be designed with independent, redundant data communication lines.

- (2) Intrusion detection and assessment must meet vulnerability assessment requirements.
- (3) The video signal must be protected based on the classification level. Video signal protection would include video signal encryption for conditions wherein video coverage cannot be masked from viewing classified matter.
- (4) IDAS must function effectively in all environmental conditions and under all types of lighting conditions or compensatory measures must be implemented.

7. PERIMETER INTRUSION DETECTION AND ASSESSMENT SYSTEM (PIDAS).

- a. Exterior IDS. The location of communication lines must be documented in the SSP consistent with Table 1, Line Supervision Protection. PIDAS must use multilayered, complementary intrusion detection sensors consistent with the vulnerability assessment.
- b. Detection Capability. A security area PIDAS must be capable of detecting an individual crossing the detection zone walking, crawling, jumping, running, or rolling at speeds between 1 to 16 feet (0.15 and 5 meters) per second or climbing the fence, if applicable, at any point in the protection zone with a detection probability of 90% and at a 95% confidence level.
 - (1) When calculating sensing probability for multiple sensor systems, detection is assumed if any of the sensors report an intrusion.
 - (2) Additional operability and effectiveness testing must be conducted and documented in the SSP (see DOE M 470.4-1, Chg. 1, *Safeguards and Security Program Planning and Management*, dated 3-7-06).
- c. PIDAS. The PIDAS surrounding the Protected Area must be monitored in a continuously manned central alarm station and a secondary alarm station. PIDAS must be:
 - (1) designed to cover the entire perimeter without a gap in detection, including the walls and roofs of structures situated within the designated security area;
 - (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 prevent adversaries from circumventing the detection system;

- (4) systems installed after July 15, 1994 must, where economically feasible, use redundant, independently routed, or separate communication paths to avoid a single-point failure;
 - (5) 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, or provide the equivalent detection and delay to meet the protection system effectiveness as described in the SSP; and
 - (6) 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.
- d. PIDAS 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.
- e. Early Warning Intrusion Long Range Detection. Sites may use early warning intrusion detection to supplement their PIDAS as a means of achieving increased adversary detection and improved overall system performance. The false and nuisance alarm rates, degradation, and detection area maintenance requirements of a PIDAS do not apply to early warning systems. Each individual early warning or extended range exterior intrusion detection sensor must have false and nuisance alarm rates that do not degrade the overall effectiveness of the system, including monitoring personnel's ability to assess and manage alarms, and be documented in the SSP.

Chapter XI - ALARM MANAGEMENT AND CONTROL SYSTEMS

1. GENERAL REQUIREMENTS. This Chapter establishes requirements for integrated physical protection systems protecting special nuclear material (SNM) and/or classified matter where required. When intrusion detection system (IDS) sensors are used to protect safeguards and security (S&S) interests the sensors must annunciate directly to alarm stations when an alarm is activated.
2. ALARM STATIONS. Alarm stations must provide a capability for monitoring and assessing alarms and initiating responses to S&S events.
 - a. Alarm station personnel must be knowledgeable of alarm station procedures and the emergency notification procedures and be familiar with the area being protected.
 - b. Tamper and supervisory alarms must be assessed by authorized personnel and technical/maintenance support personnel in accordance with local procedures.
 - c. 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.
 - d. 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.
 - e. Personnel manning the alarm station must possess an appropriate security clearance (i.e., Q or L) commensurate with the most sensitive interest under the protection of the alarm station.
 - f. Access control systems must ensure admission of only authorized personnel into the alarm station.
 - g. Alarms must annunciate both audibly and visibly to an alarm station.
 - h. Multiple alarms must be prioritized based on the importance of the S&S interests.
 - i. If response to an alarm activity by local law enforcement agencies/security personnel is permitted, then the alarm company/service must meet the specifications contained in Underwriters Laboratories (UL) Standard 827, *Standard for Central-Station Alarm Services*.
3. COMMERCIAL ALARM STATIONS. Commercial alarms service firms must issue a current UL certification commensurate with the contracted service and must maintain this UL certification as long as the service is provided to the facility. For the protection of classified matter UL Standard 2050, *National Industrial Security Systems for the Protection of Classified Materials*, should be implemented and a certificate issued for compliance with the UL standard.

4. GENERAL REQUIREMENTS FOR THE PROTECTION OF CATEGORY I AND II SNM. The requirements for S&S alarm management and control systems used in the protection of Category I and II quantities of SNM and installed and operational after January 1, 2008, are contained in DOE M 470.4-2A, *Physical Protection*, dated 7-23-09. This chapter establishes requirements for integrated physical protection systems protecting nuclear weapons, components, and Category I and II SNM. Facilities with Category I and II quantities of SNM, or other high-consequence targets as identified by VAs, must have a central alarm station (CAS) and a secondary alarm station (SAS). All intrusion detection system (IDS) sensors must annunciate to CAS/SAS when an alarm point is activated. Systems installed after July 15, 1994, must, where feasible, use redundant, independently routed, or separate communication paths to avoid a single-point failure. The perimeter intrusion detection and assessment system (PIDAS) surrounding the Protected Area must be monitored in a continuously manned CAS and SAS.
 - a. CAS.
 - (1) The CAS must be attended continually.
 - (2) The CAS and SAS must be physically separated.
 - (3) The CAS must be designed as a hardened post, located within a limited area (LA) or greater security area and manned 24 hours a day.
 - (4) CAS must be protected against threats as defined and documented in the Site Security Plan.
 - (5) Entryways must be controlled from within the alarm station.
 - b. SAS. 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.
 - (1) 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 events (see General Requirements above).
 - (2) The SAS may be located in a Property Protection Area.
5. CLOSED-CIRCUIT TELEVISION (CCTV) 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 used as the primary means of alarm assessment and to determine response level, the system requirements are listed below.
 - (1) CCTV systems must annunciate when the video signal from the camera is disrupted or lost.

- (2) The video subsystem must be integrated with the CAS/SAS alarm display systems.
- (3) 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.
- (4) Video recorders must be actuated by the intrusion alarm and record automatically.
- (5) Video recorder response time must be rapid enough to record the actual intrusion, be able to capture sufficient information for alarm assessment.
- (6) 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).
- (7) 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 if in a locked configuration) Pan tilt and zoom cameras may be used for surveillance.
- (8) CCTV systems must use real-time signal or near real-time transmission of camera views.
- (9) The video system must accept manual override of automatic features. This capability permits the operation of a CCTV camera associated with another event.
- (10) When CCTV systems are used, the alarm control system must be able to call the operators' attention to an alarm associated video recorder/monitor.
- (11) The video assessment must be supported by sufficient lighting or other means necessary to facilitate alarm assessment.
- (12) The picture quality must allow the operator to recognize and discriminate between human and animal presence in the camera field of view.

Chapter XII - ENTRY/EXIT SCREENING

1. GENERAL. Inspections are mandatory in Protected Areas (PAs) and Material Access Areas (MAAs). Random inspections are to be conducted at other designated security area boundaries. The cognizant security authority (CSA) must determine the locations and scope of the screening program at other than PA and MAA boundaries. An inspection program is to deter prohibited and controlled articles being brought into U.S. Department of Energy (DOE) facilities. All personnel, vehicles, packages and hand-carried articles are subject to inspection at security areas. These programs are to protect Department assets and interests from unauthorized removal without management authorization. Any entry/exit inspection program must be documented in a Site Security Plan (SSP) or procedure.
 - a. Passage of individuals, vehicles, and/or packages or mail through entry control point inspection equipment must be observed and controlled by trained designated personnel.
 - b. Inspection equipment can include handheld and/or portable detectors, metal detectors, special nuclear material (SNM) detectors, explosive detectors, and x-ray systems and must assist security personnel in ensuring that prohibited and controlled articles will be detected before being brought into or removed from DOE facilities.
 - c. Entrance inspections of personnel, vehicles, packages, and hand-carried items must be performed to deter and detect prohibited and controlled articles.
 - (1) Bypass routes around inspection equipment must be closed or monitored to deter unauthorized passage of personnel and hand-carried articles.
 - (2) Measures are to be instituted to correctly maintain control settings on all entry/exit control point inspection equipment.
 - (3) Equipment, to include portal monitors, must have audible and visual alarms monitored by on-post trained personnel.
 - (4) Ingress/egress points must be designed to preclude commingling of searched and unsearched personnel.
 - d. Passage of individuals, vehicles, and/or packages or mail through entry control points must be inspected prior to entry. Hand-held and/or portable detectors, etc. must be available to resolve alarms and be available for use during inspection equipment failures.
2. ENTRY INSPECTIONS. Metal detectors used for entry inspection must detect test weapons listed in Chapter VI.

- a. Explosives Detection.
 - (1) Sites must analyze their facilities to determine the potential for an adversary to use explosives to affect consequences and show that sufficient protective measures have been implemented to reduce the risk of a successful attack. The specific location of the screening will be determined by the CSA. In any instance it must be before gaining access to a PA.
 - (2) If the analysis determines that explosive detection is required, explosive detection equipment must be able to detect explosives as identified in the SSP. The SSP must document the analysis that establishes a facility's capability to detect explosives and provides protection against the malicious use of explosives.
 - (3) Documentation must include the rationale for explosive detection equipment/systems selection, deployment, and use.
- b. Metal Detection.
 - (1) Metal detection must be used in the entry process at all designated protected area boundaries.
 - (2) X-ray machines may be used to supplement metal detectors and protective personnel hand searches for prohibited and controlled articles.
3. EXIT INSPECTIONS. Personnel, vehicles, and hand-carried items including packages, briefcases, purses, and lunch containers are to be inspected to deter and detect unauthorized removal of classified matter or other safeguards and security interests from PAs. The CSA is to determine whether the inspections will be conducted at the PA or MAA. The determination will be documented in a SSP.
 - a. SNM detectors used in the inspection process must be able to detect unauthorized removal of SNM as defined by the SSP.
 - b. SNM detectors and metal detectors must be used in a combination that precludes the opportunity to defeat the detectors individually and/or when used to inspect personnel for prohibited and controlled articles.
 - c. Metal detectors used in the exit inspection process must ensure shielded SNM is not removed without authorization.
 - d. Specific inspection procedures and the approach to responding to alarms with limitations and thresholds for SNM detectors must be established and documented in the SSP or a procedure.
 - e. Exit inspection procedures must be written to ensure the following.

- (1) Identification of detection thresholds for security interests. The thresholds must be consistent with the type, form, quantity, attractiveness level, size, configuration, portability, and credible diversion amounts of articles or property contained within the area.
 - (2) The detection of shielded SNM (e.g., by using entry control point screening system equipment in a combination that precludes the opportunity to defeat the detectors individually).
 - (3) Entry control points without the means to detect unauthorized removal of material are not used to exit except in emergencies where equivalent protection measures are implemented when emergency exits are used (e.g., searches are conducted at an assembly area).
 - (4) Explosive vapor detectors and metal detectors should be used in a combination that precludes the opportunity to defeat the detectors individually at designated area boundaries and when used to inspect personnel for explosives or other prohibited/controlled articles.
 - (5) Entry control point systems must allow the authorized entry and exit of personnel while detecting prohibited and controlled articles. Entry control point configuration must have separate material package inspection areas/stations for inspecting personnel, packages, and hand-carried items. The following design criteria apply:
 - (a) Entry/exit point inspection monitors must be collocated with designated security posts to facilitate the initiation of a response to an alarm.
 - (b) Security posts must be designed with an unobstructed view or camera coverage to facilitate observation of any attempt to bypass systems.
 - (c) PA/MAA entrances/exits must be equipped with intrusion detection (either in the entrance/exits) sensors or controlled at all times to notify of unauthorized use.
- f. Emergency Personnel and Vehicles. Emergency personnel and vehicles may be authorized for immediate entry to the PA in response to an emergency if conditions and procedures for immediate entry are documented in the SSP.
- (1) The protective force or other designated site personnel must maintain continuous surveillance of all emergency vehicles that enter the site.
 - (2) If the emergency condition prevents an exit inspection before departing the site, an escort must be provided, and both personnel and emergency

vehicles must be inspected as soon as the emergency is over. If an escort is not provided, provisions must be made for continuous surveillance of all emergency vehicles that enter the PA.

- (3) As described in the NNSA *Information Security* NAP, local procedures must be developed for safeguarding classified matter from inadvertent access by uncleared personnel, or cleared persons who do not have a need-to-know, during emergencies.

Chapter XIII - PROTECTION DURING TRANSPORTATION

1. GENERAL REQUIREMENTS. This Chapter defines requirements for the transportation of Category I, II, III and IV special nuclear material (SNM). Packages or containers containing SNM must be sealed with tamper-indicating devices. Category III quantities of SNM may be transported by the following methods unless otherwise prohibited by statute (see U.S. Department of Energy (DOE) O 460.2A, *Departmental Materials Transportation and Packaging Management*, dated 12-22-04). Other items of special national security interests may, on occasion, be designated for transportation safeguards system transport (see DOE O 461.1A, *Packaging and Transfer or Transportation of Materials of National Security Interest*, dated 4-26-04). Classified nuclear explosive parts, components, special assemblies, sub-critical test devices, trainers or shapes containing no fissile nuclear material or less than Category II quantities of fissile nuclear material must be shipped consistent with both DOE policy governing protection of classified information and U.S. Department of Transportation regulations governing interstate transportation.
2. CATEGORY IV QUANTITIES OF SNM. Category IV quantities of SNM may be transported by the following methods unless otherwise prohibited by statute.
 - a. Domestic offsite shipments of classified configurations of Category IV quantities of SNM may be made by the Office of Secure Transportation (OST) or by other means when approved by the National Nuclear Security Administration cognizant security authority (CSA).
 - b. 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. 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 (see DOE M 470.4-1, Chg. 1, Safeguards and Security Planning and Program Management, dated 3-7-06).
 - d. Shipments must be made by a mode of transportation that can be traced, and within 24 hours from request, can report on the last known location of the shipment should it fail to arrive on schedule.
3. CATEGORY III QUANTITIES OF SNM. Offsite shipments of Category III quantities of SNM may be transported by the following authorized methods unless otherwise prohibited by statute (see DOE O 460.2A).
 - a. Domestic offsite shipments of classified configurations of Category III quantities of SNM must be made by OST or by an OST-approved commercial carrier that meets the requirements listed in paragraph 2b(1) below.

- b. Offsite shipments of unclassified configurations of Category III quantities of SNM are not required to be made by OST. If OST is not used, the shipments may be made by the following means:
 - c. The following requirements must be met. Government-owned or exclusive-use truck, commercial carrier, or rail may be used.
 - (1) Transport vehicles must be inspected by security personnel before loading and shipment. Cargo compartments must be locked and sealed after the inspection and remain sealed while en route.
 - (2) Shipment escorts must periodically communicate with a control station operator. The control station operator must be capable of requesting appropriate local law enforcement agency response if needed.
 - (3) No intermediate stops are permitted except for security interests.
 - d. Air shipments must be under the direct observation of the authorized escorts during all land movements and loading and unloading operations. Movement between security areas at the same site must comply with the locally developed and approved shipment security plan.
4. OFFSITE SHIPMENT OF CATEGORY I AND II SNM. Offsite shipment of fissile nuclear materials of national security interest Category I and II quantities of SNM must be transported within the Transportation Safeguards System as addressed in DOE O 460.2A. Specific items included in this policy are nuclear explosives, nuclear explosive components, special assemblies, sub-critical test devices, trainers, bulk fissile nuclear materials, and truck-transported naval fuel elements.
5. ONSITE SHIPMENT OF CATEGORY I AND II SNM. Movements of SNM between protected areas at the same site or between protected areas and staging areas on the same site must be escorted by armed protective force officers.

ATTACHMENT 1 – DOE SECURITY BADGE PROGRAM

1. GENERAL REQUIREMENTS. U.S. Department of Energy (DOE) security badges issued to Federal and contractor employees have been determined to be the Department's Federal Agency identity credential. Within the DOE, a Homeland Security Presidential Directive-12 (HSPD-12) credential, hereafter referred to as the DOE security badge, must be issued to and worn by all DOE and contractor personnel (cleared and specified unclassified personnel, as further detailed below) who require access to DOE facilities. The DOE security badge is to replace the existing DOE standard security badge. Existing DOE standard security badges may be used until the new DOE security badge has been completely implemented within DOE. The DOE implementation of the new DOE security badge requirements are based on the Personal Identity Verification (PIV) guidance issued by DOE Notice or its successor (see DOE N 206.4, *Personal Identity Verification*, dated 6-29-07). A local site-specific only (LSSO) badge is permitted for local site use. The Office of Science (SC) badge may only be used at specified SC facilities by unclassified contractors. The LSSO and SC badges do not replace the DOE security badge.
 - a. DOE Badges. The following requirements apply.
 - (1) DOE security badges must be issued to all Federal employees and cleared contractor employees and all DOE Headquarters (HQ) contractor employees who require long-term (greater than 6 months) access to DOE facilities or who have, or must have, a security clearance.
 - (2) LSSO badges may be developed and issued to address a variety of issues and unique local badging requirements including local site-specific access badge, temporary visitor badge, SC badge, foreign national badge, etc. These badges are not HSPD-12-compliant and are not recognized as meeting the requirements of the new DOE security badge.
 - (3) Specifications for the new DOE security badge are described in National Institute of Standards and Technology (NIST) 800-104, *A Scheme for PIV Visual Card Topography*. The identity verification and issue process is described in a DOE Notice or its successor (see DOE N 206.4).
 - (4) Individuals who are awaiting an L or Q security clearance may be badged using a LSSO badge. Once the security clearance is granted, the individual must be issued a new DOE security badge.
 - (5) Employee identification cards must not be substituted for the new DOE security badge or any of the site-issued or foreign national badges.
2. TYPE OF DOE BADGE.
 - a. DOE Federal and Contractor Employee Badges.

- (1) New DOE security badges must be issued to DOE and contractor employees (including subcontractors) who have been granted a security clearance and who require access to DOE security areas or who have been subjected to an HSPD-12 identity verification and suitability determination. These badges must be used and accepted at all DOE sites and facilities (see DOE M 470.4-5, *Personnel Security*, dated 8-26-05).
- (2) Badges must be approved and authorized by the sponsoring site: Federal or Maintenance and Operations contractor organization/badging authority maintaining the badge holder applicant's identity documentation. DOE Agreements with other Federal departments and agencies for the processing, replacement, and turn-in of the HSPD-compliant DOE security badge have been established in order to fulfill the HSPD directive. These arrangements must be documented in a procedure to include the provisions for the protection of the personal information.

b. LSSO Badges.

- (1) LSSO badges may be developed and issued to address a variety of local issues and unique badging needs as identified in local procedures approved by the cognizant security authority (CSA). This would include subcontractors who do not require a security clearance or access to a DOE site or facility for more than 6 continuous months, without limitation on the contract performance period.
- (2) LSSO badges include visitor badges, vendor badges, provisional badges, foreign national badges, and other site-specific badges designed and implemented to meet local requirements.
- (3) Military and other Federal department and agency personnel who possess HSPD-12 credentials/badges issued by their respective organizations and who are assigned/detailed to DOE will be issued a LSSO badge.
- (4) CSA must prescribe or approve procedures for the design, issuance, use, accountability, and return of LSSO badges. LSSO badges must not resemble the design or color of the new DOE security badge or the DOE standard security badge.

c. Visitor Badges.

- (1) Military and other Federal department and agency personnel who possess HSPD-12 credentials/badges issued by their respective organizations may, at the discretion of the NNSACSA, be permitted entry to a property protection area (PPA) without further badging. If there is a requirement for entry beyond a PPA or access to special nuclear material (SNM), nuclear weapons, or classified matter, the provisions of paragraph 2.c(3) below must be followed. Even though the person possesses an HSPD-12

credential/badge, issued by another Federal department or agency, the DOE visitation process must be followed.

- (2) Cleared visitors may be issued an LSSO badge if they possess a Q or L DOE security clearance or a Top Secret or Secret clearance granted by another Federal department or agency. Individuals with valid HSPD-12 credentials do not require re-badging with DOE HSPD-12 badges. Temporary/LSSO badges may be issued, if necessary. Classified visits must be conducted in accordance with the requirements of DOE M 470.4-1, Chg. 1, *Safeguards and Security Program Planning and Management*, Section L, *Control of Classified Visits Program*, dated 3-7-06. Before badge issue, the status of clearance must be validated with the granting department or agency.
 - (3) Military or other Federal department and agency personnel who are visitors not provided with new DOE security badges or their department's or agency's HSPD-12 credentials must follow the visitation procedures of the site to be visited.
 - (4) Visitors possessing a security clearance who require access to a Limited Area (LA), Protected Area (PA), and/or Material Access Area (MAA), SNM, nuclear weapons or classified matter must submit a DOE F 5631.20, "Request for Visit or Access Approval" (DOE M 470.4-1, Chg. 1) prior to arriving at the Site.
- d. Temporary Badges. Temporary badges may be issued to DOE and DOE contractor employees under locally approved procedures. Temporary badges must not resemble the DOE security badge and the DOE standard security badge. Temporary badges must clearly indicate that the badge is temporary.
- e. Foreign National Badges. Badges issued to foreign nationals will have a blue horizontal name bar with the individual's name printed on the blue name bar background. The badge should be processed as follows:
- f. Cleared Foreign Nationals. Cleared foreign nationals may be issued DOE security badges. The difference between the cleared foreign national badge and the DOE security badge issued to U.S. citizens is that the individual's name will be printed on a blue name bar.
- (1) The foreign national security badge must be approved and authorized by the organization/badging authority holding the foreign national's personnel clearance file.
 - (2) Cleared foreign nationals must adhere to the requirements in DOE O 142.1, *Classified Visits Involving Foreign Nationals*, dated 1-13-04 (see DOE M 470.4-1, Chg. 1).

- (3) A foreign national may be badged at a DOE security clearance equivalent to their country's approved access level. The equivalent security clearance level should be based on the Government-to-Government Agreement and official validation by the foreign government of the person's clearance (see DOE O 142.1).

NOTE: If there is no equivalent DOE security clearance level, the foreign national is badged as uncleared.

- (4) When a cleared foreign national with a DOE security badge, which is marked with a security clearance identifier, needs to access another DOE facility, the foreign national visit must adhere to the requirements of DOE O 142.1 and the provisions of DOE M 470.4-1, Chg. 1.

g. Uncleared Foreign Nationals. Uncleared foreign nationals whose official duties require routine or regular access to DOE facilities must be issued LSSO badges.

- (1) A foreign national badge may be issued for unclassified site access after an identity verification process has been completed by the foreign visits and assignments staff of the organization sponsoring the visit.
- (2) Uncleared foreign nationals must adhere to the requirements in DOE O 142.3, Chg. 1, *Unclassified Foreign Visits and Assignments Program*, dated 2-21-08 (see DOE M 470.4-1, Chg. 1).

h. Emergency Responders. Emergency responders, designated by their organizations, will be issued DOE security badges. The badge will have the words "Emergency Response Official" printed on a red horizontal background.

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

a. Security Badge Issue. The CSA must prescribe local procedures for issuance, use, accountability, and return of DOE security and LSSO badges. These procedures must address the transition from the current DOE security badge to the new DOE security badge.

b. Issuer Requirements.

- (1) Issuance with SNM or Classified Access. Measures must be taken to ensure that a single individual cannot process and/or issue a DOE security or LSSO badge allowing unauthorized access into an area containing SNM or classified matter.
- (2) Issuer Clearance Level. Issuing personnel with read/write access to systems containing records and information concerning badges, security clearance, and access control authentication data must be cleared at the appropriate level as determined by the site and documented in local

procedures. Sites must implement procedures to control access to security systems that maintain badging and clearance information.

- c. Site Usage. A valid DOE badge with a printed “L” or “Q” must be used and accepted as evidence of security clearance 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 security clearance level and determining need-to-know before granting access to SNM or classified information.
 - (2) The information on the electromagnetic stripe, optical, or other data storage media must not be used for any purpose other than physical security and logical access control. The information on the electromagnetic stripe, optical, or other data storage media or in combination with biometric access control devices must not be collected or stored outside of DOE access control applications, without prior authorization along with established procedures for the control and protection of the information.
- d. Thirty-Person Operations.
- (1) DOE security badges must be worn at DOE facilities and operations involving access of 30 or more Federal and contractor employees and who require a security clearance or who support DOE HQ.
 - (2) Facilities and operations involving fewer than 30 persons whose contractor personnel do not require a security clearance or support DOE HQ are not required to have a DOE security badge. However, when uncleared personnel need access to a DOE site, building, or location other than the HQs facilities, for no more than 6 months an LSSO badge may be issued.
- e. Recovery of DOE Badges.
- (1) DOE security badges are the property of the U.S. Government. Local procedures must be established for returning badges to the issuing office whenever an individual has terminated employment or their security clearance status changes or otherwise no longer requires the badge.
 - (2) 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 CSA.
 - (3) 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 and the records so annotated.

- (4) If a terminated employee's DOE security badge is not recovered on the last day of employment steps must be taken to recover the badge. If the badge is not recovered, the badge must be treated as stolen Government property and reported in accordance with the DOE M 470.4-1, Chg. 1, *Safeguards and Security, Program Management and Planning*, Section N, *Incidents of Security Concerns*, dated 3-7-06.
 - f. 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.e., no longer resembles the person in the photograph.
 - g. Badge Destruction. DOE security badges that are deactivated or 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. DOE security badges must be destroyed in a manner approved by Federal Information Processing Standard (FIPS) FIPS-201-1, *Personal Identity Verification of Federal Employees and Contractors*.
 - h. Temporary and Visitor Badge Reuse. Temporary and visitor's badges that do not include individuals' photos must be recovered and may be reissued unless otherwise established by the CSA and documented in site-specific requirements and procedures.
 - i. DOE Federal and Contractor Employee Name Change. A DOE security badge must be replaced when the employee's name is legally changed.
4. ACCOUNTABILITY OF DOE SECURITY BADGES. Records must be maintained by issuing offices showing the disposition of DOE security and LSSO badges. Such records must include the description and badge number; date of issuance; and name, organization, and date of the destruction along with a destruction certificate.
 - a. Records. Records must be maintained in accordance with the requirements of the local records management program. Personal data must be protected from loss or compromise (see 5 U.S.C. 552).
 - 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 theft or loss and recovery of DOE issued security badges must be reported immediately to the issuing office.
5. PROTECTION OF DOE BADGE MATERIALS AND EQUIPMENT. Stocks of badging materials, unissued DOE security and LSSO badges, and processing equipment must, at a minimum, be stored in a locked room, or locked filing cabinet/safe cabinet to protect against loss, theft, or unauthorized use. Security must be in place when the badge office is not located in a permanent facility. The CSA must establish protective measures for satellite facilities that are located outside a permanent facility. The CSA must provide

guidance on the protection of LSSO badge stock and processing equipment when located within a permanent and/or satellite facility. Thefts should be reported commensurate with the Incidents of Security Concern Program (see DOE M 470.4-1, Chg. 1).

6. DOE SECURITY BADGE VALIDATION. The CSA 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 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 DOE facility entry/exit.
 - b. Other methods of validation may be instituted employing biometrics or a combination of personnel verification measures.

7. DOE SECURITY BADGE RECIPIENT REQUIREMENTS. The CSA approves implementing procedures to ensure individuals receiving the DOE security or LSSO badge are responsible for the following:
 - a. Protecting the DOE security badge against loss, theft, or misuse and reporting a lost, stolen, or misused badge to the CSA within 24 hours of discovery.
 - b. 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 (other than what would be deemed official government business).
 - c. Returning the DOE security badge, according to local procedures and as approved by the CSA, when it is no longer valid or required.
 - d. Surrendering or returning the DOE security badge when requested according to local procedures approved by the CSA.
 - e. 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).

8. DOE SECURITY BADGE-HSPD-12 REQUIREMENTS. The requirements for the Federal government implementation of the HSPD- 12 credential are described in FIPS-201-1.