Table of Contents

1.0 INTRODUCTION 3

1.1 PLANNING 3
1.2 SECURITY LAYERING AND ZONING (DEFENSE IN DEPTH) 4
1.3 VULNERABILITY/RISK ASSESSMENT 5
1.4 CAPABILITY TO INCREASE OR DECREASE SECURITY 5

2.0 APPLICATION OF CHAPTER 5

3.0 ACRONYMS AND DEFINITIONS 6

4.0 PROJECT/PROGRAM MANAGEMENT 8

4.1 GENERAL 8
4.2 PROGRAM PLANNING 8

5.0 PHYSICAL PROTECTION PROGRAM REQUIREMENTS 10

5.1 MAJOR ELEMENTS 10
5.2 BASELINE PHYSICAL SECURITY REQUIREMENTS 10
5.3 BARRIERS 19
5.4 LIGHTING AND ELECTRICAL POWER REQUIREMENTS 27
5.5 INTERIOR INTRUSION DETECTION AND AUTOMATED ACCESS CONTROL SUBSYSTEMS (IIDS/AACS OR IDS/ACS) 30
5.6 COMMUNICATION AND CYBER SECURITY -- PROTECTED TRANSMISSION SYSTEMS (PTS) 32
5.7 EXTERIOR SECURITY SYSTEM REQUIREMENTS (PIDAS) 41

6.0 APPENDICES 41

RECORD OF REVISIONS

Rev	Date	Description	POC	Resp. Mgr.
0	5/17/2006	Initial issue. Supersedes similar material in Ch 7 Sections D5030 and G4030 on PTS and PSS.	Robert Gonzales, *S-1*	Mitch Harris, *ENG-DO*
1	10/27/2006	Administrative changes only. Organization and contract reference updates from LANS transition. IMP and ISD number changes based on new Conduct of Engineering IMP 341. Master Spec number/title updates. Other administrative changes.	Robert Gonzales, *SEC-PPS1*	Kirk Christensen, *CENG*
1 Chg 1	4/02/2007	Standard Details references and links corrected to latest (2004/2005) documents.	Robert Gonzales, *SEC-PPS1*	Kirk Christensen, *CENG*
2	10/5/2009	Referenced Electrical Section D5030 for server room cooling and monitoring at 5.2.H.7 and 5.6.D.1 and E.1; other admin changes.	Robert Gonzales, *PS-1*	Larry Goen, *CENG*

Contact the Security Standards POC
for upkeep, interpretation, and variance issues

Section F1033	**Security POC and Committee**

1.0 Introduction

This chapter establishes general security standards for use when planning and designing new or modifying existing facilities for which security is a concern. The standards in this chapter are intended for use during the early stages of facility design or modification planning. As the facility planning and design process progresses, site-specific security requirements not available in this standard must be integrated.

The objectives, guiding principles and core functions of ISSM are incorporated into this document. Integrated Safeguards and Security Management (ISSM) is a formal, organized process used throughout the DOE complex for planning, performing, assessing and improving the secure conduct of work in accordance with risk-based protection strategies.

Physical security requirements for facility planning, design, and construction are determined by identification of the Design Basis Threat and implementation of established protection strategies. The protection strategies typically provide for defensible layers. Each layer is designed to be a ring of consistently applied security measures. These layers, or "rings of defense," usually begin at the site perimeter and access control points, and step inwardly to facility exteriors and designated interior zones and control points. The security protection strategies used for each specific facility are based on threat assessments and vulnerability studies performed during early facility planning. Subsequent security planning efforts should begin with appropriate site selection and should consider stand-off and distance as a means of minimizing security requirements within the site perimeter and access control points. Additionally, security planning efforts should identify security requirements and systems to be included in the facility design. In this way security costs can be identified and managed through out the life cycle of the project.

Organization: This chapter is organized beginning with definitions of Security Areas, followed by high level facility requirements for classified materials that are in use and in storage, a list of the major physical protection elements, and then detailed descriptions of the physical security construction requirements for each Security Area. More detailed information for each physical security construction element, e.g., lighting, access controls, intrusion detection, and so forth, is included in Section 5.

1.1 Planning

Just as building codes and the American with Disabilities Act have become part of the design vocabulary, so should security and safeguards design principles. To ensure the design and construction of safe, secure and cost effective facilities, security planning must be an integral part of the overall building and site planning process at LANL.

As with planning and building sustainable facilities at LANL, the impacts and requirements of Safeguards and Security should be considered in the Whole Building Design Process.[1] The whole-building design process is a multi-disciplinary strategy that effectively integrates all aspects of site selection, site development, building design, construction, operations and maintenance. From a security standpoint, the use of the Whole Building Design process minimizes security costs and will ensure appropriate levels of protection are implemented. The Requirements Integration Team (RIT), a multi-disciplinary team of SMEs, uses a graded approach to determine the appropriate security design criteria for each project based on a facility-specific risk assessment and an analysis of all available information on security considerations, constraints, and tenant needs.

[1] WBD approach explained at http://www.wbdg.org/wbdg_approach.php

Table 1.1, Site Security Planning Elements, below, shows elements typically considered when determining security requirements for a facility site.

Table 1.1
Security Site Planning Elements

1. Topography and vegetation
2. Adjacent properties and operations
3. Parking and vehicular access
4. Pedestrian access
5. Surrounding roadways and vehicular entries
6. Existing structures
7. Fencing
8. Sight lines and visibility
9. Vegetation, visual obstructions, and potential hiding places
10. Site utility access
11. Existing or proposed infrastructure
12. Existing physical and technical security

1.2 Security Layering and Zoning (Defense in Depth)

Security layering and zoning is a protection strategy which provides protection concepts, systems, and tools for facility design and construction. Security layering defines the defensive elements of facility in three primary elements; starting with the site perimeter, the facility and building envelopes, and moving toward the interior of the building. Each layer provides an ever-increasing level of security which will be dictated by the level of security assets to be protected. This is often referred to as defense-in-depth.

Table 1.2
Building Security Considerations/Layering

1. Activities, operations, and tenant mix
2. Circulation, life safety systems, and egress requirements
3. Exterior envelope construction and glazing systems
4. Structural systems
5. Infrastructure locations and distribution
6. Space planning and program adjacencies
7. Air intakes and vents
8. Exterior doors and accessibility
9. Roofs and accessibility
10. Lobbies
11. Loading docks
12. Security operations and building control centers
13. System redundancies

14. Vehicle standoff
15. Perimeter systems
16. Vehicle access control systems
17. Pedestrian access control systems
18. Specialized security equipment

1.3 Vulnerability/Risk Assessment

The early analysis of vulnerabilities and risk ideally will establish security design and cost requirements prior to approval of CD-0 (Conceptual Design) by senior LANL and DOE/NNSA management. Security design requirements will vary depending on the levels of protection required and the physical barriers or systems required to meet the selected protection strategy. These strategies and systems will be identified by the Security Requirements Integration Team (RIT) as a result of their review of Functional and Operational Requirements for each project and as the result of any facility or project risk/vulnerability assessment which may be required.

Vulnerability/Risk Assessments have become a critical part of the design process both in existing and new LANL facilities and buildings. Although assessments are not new to the design process, the need for assessment has become better defined and in some cases has been mandated by DOE/NNSA as a result of several well known attacks on federal facilities. (Currently DOE Order 413.3, Program and Project Management for the Acquisition of Capital Assets, requires a preliminary vulnerability analysis for projects requiring Capital Acquisition of $5M or greater).

The LANL Vulnerability Analysis Group (SAFE-2) performs Vulnerability Assessments (VAs) and analyses. In doing so, the VA team identifies facility assets; threats; threat capabilities; facility and operational protection characteristics; and provides risk analyses in report form to offer recommendations for further risk mitigation. The PS-1 maintained Risk Assessment Process Guide, September, 2005, provides guidance for these analyses and is based on the requirements of DOE M 470.4-1 and DOE O 470.3A.

1.4 Capability to Increase or Decrease Security

Since the Design Basis Threat may change over the life of a facility, building owners and managers should be aware that the security elements can be more economically integrated within structures during the early planning and design phases of new construction projects than during subsequent additions or renovations. Retrofits of existing facilities pose a greater challenge because building systems must be able to accommodate increased requirements and may not have the additional space or compatibility to upgrade systems capabilities. Designs should include the ability to increase security in response to a heightened threat, as well as to reduce security if changes in risk warrant it.

2.0 Application of Chapter

2.1 This chapter helps ensure that all construction projects at LANL will be designed and constructed to provide adequate protection for their occupants and contents against terrorist threats and other malevolent acts and will also provide the required levels of security for activities, materials and/or documents within the facility as may be dictated by DOE requirements and regulations.

2.2 This chapter provides for the design of adequate protection measures for each new or remodel facility project based upon a Design Basis Threat established for each facility.

2.3 This chapter establishes a system for determining the level of security features required for each facility, and will guide the user in selecting and designing cost effective security features adequate for protection

from the established threat which are also efficient, convenient, maintainable, standardized, and adequate for future expansion.

2.4 This chapter provides requirements and guidance that applies to the design and construction of new facilities and remodel or modification of existing facilities.

2.5 Use this chapter in conjunction with ESM Ch 1 Section Z10, *General Requirements for All Disciplines*, and other interfacing ESM chapters. For administrative access control (simple property protection) use ESM Chapter 7 Electrical, Section D5030.

2.6 Guidance is indicated by section titling or italics (expect where used to set off document titles as was done in paragraph above).

3.0 Acronyms and Definitions

AACS	Automated Access Control Subsystem; works in conjunction with Interior Intrusion Detection Subsystem to provide electronic protection of assets. Same as Access Control Subsystem (ACS)
AFP	Argus Field Panel (or processor), the most modern type of processor in an Intrusion Detection/Access Control subsystem.
AIS	Automated Information System
AT/FP or ATFP	Anti Terrorism/Force Protection. A term in current use within the design and security professions to broadly refer to design concepts and requirements used in the design of facilities deemed to be at risk of terrorist or other attack.
Category I, II, III, IV	DOE category for amounts of Special Nuclear Material, with Cat I the highest.
CDIN	Classified Distributive Information Network. Any cable, wire, or other approved transmission media used for the clear text transmission of classified information in certain DOE controlled access environments. Excluded is any system used solely for the clear text transmission and reception of intrusion/fire alarms or control signaling. **CDIN-1:** Type of CDIN used in a Limited Area **CDIN-2:** Type of CDIN used in a Property Protection Area
Central Alarm Station (CAS)	Used in the protection of Category I and Category II quantities of special nuclear material. Meets the requirements of a hardened post and is located, as a minimum, within a Limited Area.
Concentric Security Area	With the exception of a Material Access Area, this is a security area within a larger Security Area.
CSSM	Cyber Security Site Manager in Chief Information Office (OCIO) -- PTS, etc. Formerly S-11.
Design Agent or Design Agency	The organization performing the detailed design and analysis of a project or modification.
DBT	Design Basis Threat
ECP	Entry Control Point
ESM	Engineering Standards Manual, PD 342
Exclusion Area (EA)	A Security Area defined by physical barriers and subject to access control, where mere presence in the area would result in access to classified matter.
Facility	Normally at LANL, facility is a synonym for Real Property and Installed Equipment. RP&IE is the land, improvements on the land such as buildings, roads, fences, bridges, and utility systems and the equipment installed as part of the basic building construction that is essential to normal functioning of a building space, such as plumbing, electrical and mechanical systems. This property/equipment is also referred to as institutional or plant and was formerly known as Class A. [from DOE Order 4330.4B]
IDA	Intrusion Detection Alarm, typically the name given to a zone protecting a Vital Area.
IIDS	Interior Intrusion Detection Subsystem. Same as Intrusion Detection Subsystem

	(IDS).
LFP	Laboratory Field Panel, the type of controller in an Intrusion Detection/Access Control subsystem that is gradually being phased out in favor of AFPs and Argus.
Limited Area (LA)	A Security Area defined by physical barriers, used for the protection of classified matter and/or Category III quantities of special nuclear material, where protective personnel or other internal controls can prevent access by unauthorized persons to classified matter or special nuclear material.
Material Access Area (MAA)	A Security Area defined by physical barriers and subject to access control, used for the protection of Category I quantities of special nuclear material or Category II quantities of special nuclear material with credible rollup to Category I quantity. A Material Access Area shall be contained within a Protected Area and shall have separately defined physical barriers constructed to provide sufficient delay time to control, impede, or deter unauthorized access. Area boundaries shall conform to the layered protection concept with a separate Material Access Area located within a separate and distinct Protected Area. Material Access Areas shall direct the flow of personnel and vehicles through designated portals.
NIJ	National Institute of Justice
NM	nuclear material
POB	Protected Outlet Box. See Terminal Connection.
POC	Point-of-contact. For the ESM Security POC and other ESM POCs see http://engstandards.lanl.gov/POCs.shtml#security
PRID	Permits and Requirements Identification System, a LANL in-house tool for projects to ensure they meet all requirements and obtain needed reviews and approvals
Project Leader	Project manager (assigned by organization), project leader (assigned by PM Division) or other designated individual responsible for the management and overall design effort of the project.
Project Manager	Individual assigned by the User/Program Office and is responsible for the project.
Property Protection Area	A Security Area established for the protection of Departmental property. A Property Protection Area may be established to protect against damage, destruction, or theft of Government-owned property. Measures taken shall be adequate to give reasonable assurance of protection and may include physical barriers, access control system, protective personnel, intrusion detection systems, and locks and keys.
Protected Area (PA)	A Security Area encompassed by physical barriers, surrounded by intrusion detection and assessment systems, and having access controls for the protection of Category II quantities of special nuclear material and/or to provide a concentric security zone surrounding a Material Access Area or Vital Area
PTS	Protected Transmission System. A term used to describe an approved data communications system that provides adequate physical safeguards to permit its use for the transmission of unencrypted classified information. **RED** is a designation applied to information systems and associated areas, circuits, components and equipment in which National Security Information (classified) is processed. (**BLACK** is the designation applied to information systems and associated areas, circuits, components and equipment in which National Security Information is not processed (unclassified). Encrypted signals are unclassified.) See also Terminal Connection. [Definition adapted from DOE M 200.1-1 by S-11, now CSSM]
PS	LANL's Physical Security Division
PS-1	LANL's Classified Matter Protection Group (physical protection, VTRs, locks, etc.), formerly S-5
PS-2	LANL's Security Systems Group (IDS, ACS, etc.), formerly SAFE-3 and S-3
PSS	The electronic Physical Security System, an obsolete term. Now considered Interior Intrusion Detection and Access Control Systems.
S&S	security and safeguards
SAFE-2	LANL Safeguards Division's Vulnerability Analysis Group

SAS	Secondary Alarm Station
SCIF	Special Compartmented Information Facilities located within Exclusion Areas
Security Area	Defined area of a facility for which physical protection is provided in a graded approach. Types include: Exclusion, Limited, Material Access, Protection, Property Protection, and Vital.
Security Coordinator	Project lead to ensure security features are incorporated into the design by coordinating with Security SMEs for design features and design reviews
SIT	Security Inquiry Team
SME	Subject Matter Expert
SNM	Special Nuclear Materials
RIT	Requirements Integration Team
SO-3	LANL's Security Operations Division Security Integration Group
SSSP	LANL's Site Safeguards and Security Plan, maintained by Security Division
STC	Sound Transmission Class, a two-digit number describing the laboratory performance of a single building element in stopping the transmission of sound.
TID	Tamper Indicating Device
TSCM	Technical Surveillance Counter Measures
TEMPEST	A nationally mandated program that studies unintentional compromising emanations from information systems, communications, and electrical pathways. The LANL TEMPEST Program Coordinator recommends and implements countermeasures to mitigate and minimize the electromagnetic emanation phenomena referencing DOE directives and guidance from the DOE Certified TEMPEST Technical Authority (CTTA).
Terminal Connection	Term used at LANL to refer to the point where the user connects to the secure communications utility (personal computer interface). Terminal connections are commonly referred to as "drops." The connection is also often referred to as a Protected Outlet Box (POB). See PTS.
Vital Area	A Security Area located within a Protected Area used for the protection of Vital Equipment. All Vital Equipment shall be contained within a Vital Area.
Vital Equipment	Equipment, systems, or components whose failure or destruction would cause unacceptable interruption to a national security program or an unacceptable impact to the health and safety of Departmental and contractor employees, the public, or the environment.
VTR	Vault-type Room

4.0 Project/Program Management

4.1 General

Responsibilities: The Project Leader is responsible for the design of LANL structures, systems, and components, and is responsible for ensuring that their Design Agent implements the stated requirements.

The Project Leader shall ensure that projects or facilities under their control receive security engineering design input at the earliest possible time in the design process. A formal Security engineering and operational review of the design shall be performed before actual construction or modification begins.

4.2 Program Planning

A. Project Initiation

1. The project manager for each project shall be responsible for initiating or requesting an appropriate review of the project for Security and Safeguards (S&S) issues. The primary vehicle for initiating this process shall be completion of a Project Questionnaire within the LANL Project Review and Requirements Identification System (PRID). This system is an on-line project information gathering and analysis system. The PRID provides a specific area for assessment of project S&S requirements.

2. The Requirements Integration Team (RIT) will review the PRID security input data. If the project will involve security issues which may require specific engineering and architectural design features, the RIT will assign a Security Point-of-Contact[2]. The POC will be assigned to the Project Team as the primary S&S contact for security reviews and design input.
3. Complex projects which may involve extensive preplanning and conceptual design before a PR-ID is created and submitted my be submitted directly to the RIT. In this case the RIT will assign a project Security POC to assist with identification of security issues and needs during the project scoping, engineering study and/or conceptual design phases of the project.
4. After review of the PR-ID information submitted, if necessary, the project Security POC will forward an S&S Questionnaire to the Project Manager to collect additional information about the Project. The Project Manager will insure that the form is completed and that the form is returned to the RIT.
5. The Project's Security POC will distribute the collected project S&S information to the LANL security community to insure that an appropriate review of all S&S aspects of the proposed project is completed.
6. A risk assessment will be done for each project submitted to the RIT. The risk assessment will consider whether or not regulatory requirements such as storage or handling of special nuclear material (SNM) or of classified materials will require security improvements. Additionally, the risk assessment will analyze the risk to the facility and its occupants from an anti-terrorism/force protection (ATFP) standpoint.

B. Project Categorization

1. After review of the project data is complete, the Security POC and/or the RIT will determine the Security Level Category for the proposed project.
2. Projects assigned to the low security level category will be referred to the appropriate Division Security Officer for the owning/tenant organization(s) and that person shall become the primary security point of contact. Projects found to have a high or medium security categorization will be further analyzed to determine what level of security analysis will be required (e.g. risk assessment, vulnerability assessment.)
3. If this review indicates that significant security improvements or design features will be required (e.g., construction of a SCIF or VTR), then a project specific S&S requirements integration team will be created and appropriate security Subject Matter Experts (SMEs) will be assigned to the team to work with the LANL Project Team in identification and design of the physical security requirements.
4. In addition to security improvements required by regulatory drivers, if the risk assessment indicates the facility and its occupants are at risk of malevolent attack, (e.g. perimeter security and/or stand off distances are insufficient) then an ATFP Requirements Integration Team will be created and appropriate SMEs will be assigned to the team. The SMEs will work with the project team and the design agency to identify and recommend specific design features to lower the risk or severity of consequences to the occupants from a malevolent attack against the facility.

C. Project Execution

The dedicated RIT team member(s) will assist or participate in the following project design and construction phases:

[2] Not to be confused with this chapter's POC.

1. Conceptual Design: Development of engineering studies, functional requirements, and design criteria.
2. Preliminary and Final Design: Development of preliminary and detailed design of physical security features which may be required; intermediate and final review(s) of project drawings, specifications and other contract documents which may be developed for the project.
3. Start-up and commissioning planning: Participate in the development of the Test and Acceptance Plan and/or any Commissioning Plan which may be developed for the project to insure that passive and active security systems will be inspected, tested, and accepted in an appropriate and thorough manner (ref. ESM Ch. 15, Commissioning-future).
4. Construction Phase: Conduct intermediate and final inspections of physical security features and general construction as may be required during construction of the facility.
5. Commissioning: Conduct or witness any tests of passive and active physical security features or systems as may be required by the Commissioning Plan.
6. Readiness Activities: Participate as the Project Security Representative in any Readiness Review or Assessment which may be required for the facility.

5.0 Physical Protection Program Requirements

5.1 Major Elements

There are six major elements that comprise a physical protection system. The type of security area that will be required (based on what must be protected) will determine which of these basic protection requirements must be incorporated into the planning, design and construction of the project.

Baseline Protection Requirements

- Barriers—A system of barriers or other impediments to delay, channel personnel, or deny access to SNM or vital areas.
- Intrusion Detection System—A system providing the capability to detect an adversary action or anomalous behavior.
- Assessment System—A system providing the capability to assess the nature of the adversary action.
- Communication System—A system providing the capability to communicate to response forces and other personnel.
- Response—The capability of the security organization to neutralize the adversary.

5.2 Baseline Physical Security Requirements

A. General Requirements

The following physical security requirements are applicable to construction projects and apply to all Security Areas except Property Protection Areas.

1. Access shall be controlled to limit entry to appropriately cleared and/or authorized individuals.
2. Controls shall be established to detect, assess, deter, and (in certain cases) prevent unauthorized access to Security Areas.
3. Access control requirements may be layered as appropriate for the situation.
4. Automated access control systems may be used as approved by the local cognizant Departmental authority for safeguards and security.
5. Means shall be made to deter and detect unauthorized intrusion into Security Areas. Means include use of intrusion detection sensors and alarm systems, random patrols and/or visual observation.
6. Entrance/exit inspections, as required, shall be made by protective personnel or with detection equipment designed to detect prohibited articles.

7. Clearly defined physical barriers, such as fences, walls, and doors, shall be used to define the boundary of a Security Area.
8. Barriers shall direct the flow of personnel and vehicles through designated entry control portals and shall allow for ingress and egress of emergency vehicles and fire protection equipment.
9. Barriers shall be used to deter and/or prevent penetration by motorized vehicles where vehicular access could significantly enhance the likelihood of a successful malevolent act.
10. In the case where emergency exits from Material Access Areas are not monitored, provision shall be made to assure that evacuations do not provide a theft opportunity. Emergency exists can exit into a secured outer area within a security fence which provides an evacuation or shelter area with sufficient physical separation from the structure or a pathway to such an area. Local administrative procedures can then require that the evacuation or shelter area is placed under surveillance by the protective force during any evacuation and swept with SNM detectors afterward to make sure no material has been left behind.
11. Doors that serve as exits from security areas shall with DOE security requirements, except the use of panic hardware on doors from security areas shall be limited to assembly, educational and hazardous occupancy classifications.
12. All alarm equipment must be tampered protected.
13. Security signs and postings; see Appendix A of this chapter.

B. Limited Area Requirements

A limited area is defined by physical barriers and is intended to protect classified matter and/or Category III quantities of (SNM), where protective personnel or other internal controls can prevent access by unauthorized persons to classified matter or special nuclear material.

In addition to requirements addressed above in 5.2.A, General Requirements, the following physical security requirements apply to Limited Areas and are applicable to construction projects:

1. Barriers identifying its boundaries and encompassing the designated space.
2. Clearly defined physical barriers shall be utilized to control, impede, or deny access, and shall effectively direct the flow of personnel and vehicles through designated portals, and allow effective searches. Permanent barriers shall be used to enclose security areas except during construction or transient activities, when temporary barriers may be erected.
3. Access controls to provide reasonable assurance that only authorized personnel are allowed to enter and exit the area.
4. Validation of the identity and access authorization of persons allowed access shall be administered by protective personnel (e.g., protective force or other appropriately authorized personnel) and/or automated systems at the Limited Area entrance(s).
5. A means shall be provided to detect unauthorized intrusion by use of alarm systems, random patrols, or visual surveillance.
6. Adequate protective illumination shall be provided to permit or assist in detection and assessment of adversaries, reveal unauthorized persons, and, at pedestrian and vehicular entrances, to permit examination of credentials and vehicles.

7. Measures shall be in place to prevent unauthorized visual or aural access to classified matter.

C. Exclusion Area Requirements

An exclusion area is defined by physical barriers and is subject to access control, where mere presence in the area would result in access to classified matter.

In addition to requirements addressed above in 5.2.A, General Requirements, an Exclusion Area must meet all of the requirements for a Limited Area and the following physical security requirements which are applicable to construction projects:

1. Barriers identifying its boundaries and encompassing the designated space.
2. Access controls to provide reasonable assurance that only authorized personnel are allowed to enter and exit the area.
3. Validation of the identity and access authorization of persons allowed access shall be accomplished at the Exclusion Area entrance(s) and shall be administered by protective personnel and/or automated systems.
4. Private vehicles are prohibited from an Exclusion Area.
5. Government-owned or Government-leased vehicles, and service or delivery vehicles shall be admitted only when on official business and when operated by properly cleared, authorized personnel.

D. Protected Area (PA)

A PA is encompassed by physical barriers, surrounded by intrusion detection and assessment systems, and has access controls for the protection of Category II quantities of SNM and/or provides a concentric security zone surrounding an MAA or Vital Area.

In addition to the General Requirements stated above in Section 5.2.A, the following requirements are applicable Protected Area requirements for construction projects:

1. The physical design of the PA is developed to mitigate security risks according to outside threats identified in the DOE O 470.3A, Design Basis Threat (DBT), and the design details addressing protection strategies against these treats are outlined in DOE M 470.4-2, Physical Protection. Minimal fence design height and materials are stipulated in DOE M 470.4-2, Chapter IX Section 2.
2. Intrusion detection and assessment systems shall protect in a manner consistent with the value of the property protected and the impact of loss or sabotage of the protected property and facilities.
3. A means of timely detection of intrusion shall be provided by the use of alarm systems or patrols.
4. Entrance inspections of personnel, vehicles, and hand-carried items shall be conducted to deter and detect the unauthorized introduction of prohibited articles.
5. Exit inspections of personnel, vehicles, and hand-carried items shall be conducted to deter and detect the unauthorized removal of SNM. Specific inspection procedures and special nuclear material/metal detection levels and limitations shall be established and documented.

6. A physical or electronic search shall be separately conducted of vehicles, personnel, packages, and all other containers at all routine exit points for MAAs that contain Category I quantities or lesser quantities with credible rollup to Category I quantity.
7. Exit inspections shall be capable of detecting shielded SNM (e.g., using a combination of SNM and metal detectors) and shall meet requirements for metal and SNM determined by the Manager, Operations Office.
8. Unalarmed portals without the means to detect SNM shall not be used.
9. All exits shall be alarmed or controlled at all times.
10. Adequate illumination shall be provided to detect intruders, reveal unauthorized persons, and, at pedestrian and vehicular entrances, permit examination of credentials and vehicles.
11. Armed protective force personnel and/or an automated access control system as determined by local safeguards and security authorities shall validate the identity and access authorization of persons authorized access to the area.
12. Private vehicles are prohibited from a Protected Area.
13. Government-owned or Government-leased vehicles shall be admitted to a Protected Area only when on official business and when operated by properly cleared and authorized drivers, or when escorted by properly cleared, authorized personnel.

E. Vital Area Requirements

A Vital area is located within a Protected Area and is used for the protection of Vital Equipment. All Vital Equipment shall be contained within a Vital Area.

In addition to the General Requirements stated above in Section 5.2.A, the following Vital Area requirements are applicable to construction projects:

1. Meet all of the protection requirements of a Protected Area.
2. Area boundaries shall conform to a layered protection concept, with a separate Vital Area perimeter located within a separate and distinct Protected Area.
3. The perimeter of each Vital Area shall be monitored to deter and detect unauthorized entry attempts.
4. Vital equipment shall be protected with an intrusion detection system.
5. Exits shall be alarmed or controlled at all times.
6. Validation of the identity and access authorization of persons authorized access shall be administered by armed protective personnel or an automated access control system as determined by local safeguards and security authorities.
7. Private vehicles are prohibited from a Vital Area.
8. Government-owned or Government-leased vehicles shall be admitted only when on official business and when operated by properly cleared and authorized drivers, or when escorted by properly cleared, authorized personnel.
9. Service and delivery vehicles shall be admitted only when on authorized business and when driven or escorted by properly cleared and authorized personnel.

F. Material Access Area (MAA) Requirements

A Material Access Area is defined by physical barriers and is subject to access control. It is used for the protection of Category I quantities of SNM or Category II quantities of SNM with credible rollup to a Category I quantity. The objective of the MAA boundary is to prevent or detect the unauthorized movement of material through it, while allowing for authorized personnel access, authorized material movement, and emergency evacuation as necessary.

In addition to the General Requirements stated above in Section 5.2.A, the following MAA requirements are applicable to construction projects:

1. The MAA shall be contained within a Protected Area.
2. The MAA shall have physical barriers designed and constructed to provide sufficient delay time to control, impede, or deter unauthorized access.
3. The MAA boundaries shall conform to the layered protection concept, with a separate MAA perimeter located within a separate and distinct Protected Area.
4. Designed penetrations of the MAA boundary shall either be monitored, or shall be designed and constructed so as to not provide a credible path for material removal. Penetrations shall also be designed and construction to prevent or detect any malevolent penetration of the MAA boundary.
5. MAA barriers shall direct the flow of personnel and vehicles through designated portals.
6. Entrance inspections of personnel, vehicles, and hand-carried items shall be conducted to deter and detect the unauthorized introduction of prohibited articles.
7. Exit inspections of personnel, vehicles, and hand-carried items shall be conducted to deter and detect the unauthorized removal of SNM. Specific inspection procedures and special nuclear material/metal detection levels and limitations shall be established and documented.
8. A physical or electronic search shall be separately conducted of vehicles, personnel, packages, and all other containers at all routine exit points for MAAs that contain Category I quantities or lesser quantities with credible rollup to Category I quantity.
9. Exit inspections shall be capable of detecting shielded SNM (e.g., using a combination of special nuclear materials and metal detectors) and shall meet requirements for metal and special nuclear material determined by the Manager, Operations Office.
10. Unalarmed portals without the means to detect SNM shall not be used.
11. Exits shall be alarmed or controlled at all times.
12. Access control shall be administered by armed protective force personnel and/or automated access control systems as determined by local safeguard and security authorities.
13. Validation of the identity, access authorization, and authority to enter for persons allowed access shall be accomplished at MAA entrances. (DOE M 470.4-2, Chapter V)
14. Private vehicles shall be excluded from a MAA.
15. Government-owned or Government-leased vehicles shall be admitted to MAAs only when on official business and when operated by drivers having the proper access authorization, or when escorted by personnel who have the proper access authorization.

16. Material control systems shall alert the facility to unauthorized activities. Physical barriers should be employed for containment of materials. Detection should be implemented using a variety of surveillance and monitoring techniques. A number of boundaries shall be considered to control the movement of material:
    - The boundary defined by the surface of the process equipment,
    - The boundary defined by the walls of rooms containing process equipment,
    - The boundary of the "material access area"
    - The boundary of the protected area as described in physical protection orders,
    - The boundary defined by specially constructed areas such as storage vaults.

    The reliance placed on each of these boundaries to prevent or detect the theft or diversion of material will depend on the safeguards strategy of the facility involved; however, the material access area boundary and the integrity of vaults shall generally be the most important in terms of design.
17. Walls defining the MAA boundary shall be designed or constructed so that penetration within the specified delay time is not credible. Some type of monitoring shall be provided where penetration is credible. Designs in which the walls are easily penetrated are not advisable. MAA walls shall not provide hiding places or redoubt-like structures for adversaries.
18. Penetrations in the floor and ceiling for piping, heating, venting, air conditioning and other support systems shall not be large enough or accessible enough to create credible paths for the removal of material. As with walls, ceilings should not provide places to hide material.
19. Portal systems shall allow for the passage of personnel while detecting the presence of nuclear material and metal. Equipment or package portals may be used so that tools and packages can be monitored separately.

G. Concentric Security Area Requirements

A concentric security area is an area within a larger Security Area, (with the exception of a Material Access Area, which has other physical security requirements).

1. If inspections conducted at the outer Security Area boundary are at the same level as required for the inner Security Area boundary additional entry/exit inspections are not required at the inner Security Area perimeter.

H. Vault and Vault-Type Room (VTR) Requirements

In addition to the General Requirements stated in Section 5.2.A, VTRs designed to protect classified material shall be designed and constructed to be penetration resistant. VTRs shall normally be windowless and without skylights. They shall have a combination-locked steel door and shall be protected by an intrusion alarm system. As a minimum, the following design and construction criteria are required.

1. Physical relationships should be considered in determining locations of vaults, processing areas, and shipping/receiving areas as materials will flow from one of these to the other.
2. Walls, floor, and ceiling shall be constructed of materials that afford penetration resistance at least equal to that of 8-inch think reinforced concrete.
3. Openings greater than 96 square inches in area and over 6 inches in the smallest dimension shall be protected by imbedded steel bars at least 5/8 inches in diameter on 6-inch centers both horizontally and vertically.

4. A combination locked steel door shall be provided. For new structures the door must meet Class 5 standards as set forth in FS AA-D-6008 of the Federal Specifications and Standards cited in 41 CFR 101. Doors in existing structures shall be at least 1-inch think exclusive of bolt work and locking device.
5. Doors, hardware, locks, and, where necessary, windows shall meet the security-related criteria listed in DOE O 6430.1A Division 8, Doors and Windows. In addition, doors shall comply with UL 155 and UL 10A. For a vault not containing SNM, the type of door and frame complying with Class 5 Standards of FS AA-D-600B shall be the required level of physical protection.
6. Where Substantial Construction is required, vault enclosure (walls, floors, and roofs) shall provide, as a minimum, a penetration delay time equivalent to that provided by monolithic concrete at least 8 inches thick, reinforced vertically and horizontally with not less than 5/8-inch diameter steel reinforcing bars at not more than 6 inches on center. Pre- engineered metal buildings or other similar building systems shall not be used for substantial construction unless designed, constructed, and tested for the specific purpose.
7. Vault-type rooms shall be of fire-resistant construction. Fire detection and suppression systems appropriate to the hazards involved shall be provided. For VTRs and SCIFs where design calls for the VTR or SCIF to house computer, servers, and other electronic equipment capable of increasing the heat loading within the room refer to ESM Chapter 7, Section D5030 for determination of need or design guidance for temperature sensors, thermostats, and related components. This section provides HVAC load density requirements for VTRs and SCIFs housing server equipment.
8. VTRs shall be protected with a DOE-approved IDS. The IDS shall be activated by any penetration of walls, floors, ceilings, or openings, or by motion within the room, and shall meet Fed Std W-A-450 or be approved by the cognizant DOE security authority.
9. When electronic alarm systems are used to protect classified matter or SNM, they shall also be designed to meet site-specific protection needs.
10. Intrusion alarm systems shall have a primary and auxiliary power source. Switch-over to the auxiliary power source shall be automatic. An alarm condition shall be indicated at the monitor station on failure of the primary power source(s).
11. Alarm lines shall be continuously supervised so as to detect any attempt to bypass the alarm system surreptitiously by shorting, opening, or substituting a bogus signal for the legitimate "no alarm" signal.
12. Material waiting processing shall be stored in accordance with a graded management system which establishes appropriate access controls. Facilities shall be designed to minimize the amount of attractive material and duration of storage for SNM temporarily held in accessible locations. Vaults containing attractive material should prevent hands-on access to material as much as possible. If practicable, vault design should emphasized automated material handling as this limits hands-on access and provides automatic documentation of material movements. Other strategies, such as locked carts, may be used for short-term storage of less attractive material.
13. Containment of Material in Process or Transfer:
    - Material Transfer and Process Systems equipment should provide engineered barriers to the unauthorized acquisition of attractive material. Maximization of engineered barriers can enhance or supplement other material containment strategies.
    - Areas where materials can be accessed directly (e.g., load-out areas) should be minimized in order to minimize the need for administrative controls, such as compliance with two-person control procedures.
    - Electronic surveillance systems such as Closed Circuit TV shall be considered for use in sensitive areas such as load-out stations and transfer locations.

- When electronic surveillance systems are used, adequate lighting and appropriate fields-of-view shall be provided. Areas where an individual could work unobserved are not permitted.

I. Secure Conference Room Requirements

Secure Conference Rooms are those where classified information is discussed on a recurring basis.

1. General conference rooms where classified information is discussed on a recurring or routine basis shall provide acoustical security commensurate with the guidelines outlined in DOE M 470.4, Section E, Chapter IV.
2. The secure conference room envelope, consisting of walls, floors, ceilings, doors, door frames, windows, and penetrations such as hardware, ducts and grills, transfer grills, pipes, electrical conduits, luminaries, and electrical devices and equipment shall be constructed and/or installed in accordance with guidelines established in DOE M 470.4-2, Chapter XI.
3. Based on project specific requirements, the maximum expected sound levels to be generated within a secure conference room shall be used for the design of the acoustic security features.
4. Based on the project-specific criteria, either an independent heating-cooling system with minimal utility service penetration through the room envelope shall be specified, or special sound attenuation devices shall be provided in the central heating-cooling system components in and around the conference room. These Systems should reduce airborne or structure-borne sound transmission paths. Suitable sound traps which may be used include, but are not limited to:
   - Metal air duct isolation fittings and insulation material on the secure side of the ducting.
   - Packing around pipe penetrations with fixed pipe flanges on both sides of the penetrations if appropriate.
5. Personnel access barriers/controls for exterior ductwork or other security devices shall be specified and designed as required and directed in the DOE project criteria.
6. The installation of telephones and other communication systems in conference rooms is highly discouraged. If telephones or other communication systems are provided they shall be equipped with jacks or other disconnecting devices to allow for disconnection during classified discussions.

J. Secure Office Requirements

Secure offices are those where classified information is used or discussed on a recurring or routine basis.

1. Walls, ceilings and doors of offices or rooms constituting security area perimeters where classified information is discussed, handled, or processed on a recurring or routine basis shall be constructed of materials of low sound conductivity, or shall otherwise be acoustically treated in accordance with DOE M 470.4-4 Chapter IV. These features shall be designed to prevent a person outside the room with reasonable access to the wall from overhearing a conversation at normal level within the room without the use of hearing instruments or equipment.
2. Telephones or other communication systems in offices in which classified discussions occur should be equipped with jacks or other disconnecting devices to allow for disconnection during classified discussions.
3. The secure office envelope, consisting of walls, floors, ceilings, doors, door frames, windows, and penetrations such as hardware, ducts and grills, transfer grills, pipes, electrical conduits, luminaries, and electrical devices and equipment shall individually and together provide a sound transmission

loss that leaves the sound from the secure office a minimum of 15db less than the expected background sound outside the room.

4. The maximum expected sound levels to be generated inside the secure room shall be used in the design of the acoustic security features.
5. The secure room envelope shall have a Sound Transmission Class (STC) of not less that 45 in accordance with ASTM E413. Envelope materials, components, and assemblies shall be tested by a recognized testing agency to determine their acoustical performance.

K. Technical Surveillance Counter Measures (TSCM)

1. Based on established criteria, some areas may require TSCM service. Laboratory TSCM SMEs will conduct evaluations to include involvement in pre-construction planning and site inspections during construction.

L. TEMPEST and Transmission Security

1. The LANL TEMPEST Program Coordinator must be included in all facility pre-construction planning/design activities when classified information processing in the proposed facility is planned/expected.
2. TEMPEST or Transmission Security requirements may exceed the specifications given in this standard.
3. Security measures implemented to satisfy TEMPEST or Transmission security requirements are recommended by the LANL TEMPEST program coordinator and approved by the DOE-Certified TEMPEST Technical Authority (CTTA).

M. Security Inspector Posts

1. Provisions shall be designed for security inspector posts at access portals, fixed and mobile defensive positions, and guard towers. Electronic IDS Portal monitors are generally co-located with guard stations, so that an adequate response to an alarm is available. The need and location for these shall be determined on a facility-specific basis in consideration of the DOE M 470.4 series of orders, the Departmental threat guidance, and the nature of the materials and facilities being protected.
2. The guard stations serve to control the flow of personnel into the area via identification badges, etc. When this is the case, the guard station should provide an unobstructed view of the portal. Electronic communication between the guard/station and the central security station shall enable the monitoring of power, alarms, etc. Guard stations shall be designed using physical security design criteria as well.
3. Security inspector posts, both mobile and fixed, for protected areas, shall be equipped with duress systems and be designed and located in accordance with applicable requirements contained in DOE orders. Security inspector posts shall be located to provide an unobstructed view of the surrounding terrain. The exterior walls, windows, and doors shall be constructed of reinforced materials which have a bullet penetration resistance equivalent to “high-powered rifle rating” as given in UL Standard 752, Bullet-Resisting Equipment.
4. Whenever practical, containers for the storage of weapons and ammunition shall be GSA-approved weapons storage containers which are bolted or otherwise secured to the structure.

5. For guard towers that are intended to serve as fighting positions and emergency defensive positions for security inspectors, consideration shall be given to protected firing posts and provide a minimum of 60 square feet of floor area per person.
6. Routine and emergency duty fixed posts should be located so that the efficiency of routine duties is enhanced. Likely routes of adversary ingress and egress are clearly observable, and protected routes or methods of approach are available to protective personnel.
7. Routine and emergency duty fixed posts shall provide adequate human engineering so that the protective personnel occupying the posts can perform their duties efficiently. Routine duty fixed posts shall provide occupants with adequate protection from weather and temperature variations.
8. Exterior walls, windows, and doors shall be constructed of, or reinforced with, materials that have a bullet penetration resistance equivalent to the "high power rifle" rating given in UL Standard 752, Bullet-Resisting Equipment.
9. In guard towers that are intended to serve as fighting positions in alert conditions, consideration shall be given to protected firing ports, a minimum of 60 square feet of net floor area per person and exterior walls conforming to NIJ Standard 0108.01.

5.3 Barriers

A. General Guidance

Barriers that impede, delay, or in some cases essentially deny access to SNM are an important part of access control systems. Most barriers are passive, designed to require the use of special tools and high explosives to penetrate them. Sophisticated barriers have been tested against a full range of potential adversary tools and tactics. These barriers provide considerable time delay to allow sufficient response-force strength to be assembled to neutralize the adversary force. Specialized barriers have also been developed to delay or stop vehicles, aircraft, and watercraft. Some barriers have been developed that have an active component designed to further frustrate the adversary. These systems may dispense an obscuration agent, a viscous barrier, or a sensory irritant.

B. Access Control and Inspection

1. Entry Control Points (ECP) for control and inspection of vehicle and pedestrian ingress and egress are required at each security boundary access point. The number of ECP within each security boundary shall be minimized.
2. The number of ECP shall be limited so as to establish and maintain the level of integrity required by the DOE Cognizant Operations Office for secured areas.
3. ECPs shall be designed to provide positive security control over vehicular and pedestrian traffic that enters the secured area.
4. ECPs shall be structurally hardened, as necessary, to meet site-specific criteria.
5. If an Intrusion Detection Alarm (IDA) zone is required, the ECP(s) for the security areas should be located between the IDA and the inner fence if feasible. This configuration provides a continuous IDA zone across the ECP during low traffic periods.
6. Points of vehicle and pedestrian access to restricted areas shall provide the same level of physical protection as that provided at all other points along the secured perimeter. Gate hardware for security fencing shall be installed in a manner that will mitigate tampering.
7. Except where material surveillance procedures are required, portals directly protecting special nuclear material shall permit entry of only one person per request. If no emergency portals are available in the secured area, portals shall be capable of permitting unimpeded ingress by authorized emergency personnel.

8. Automated access control systems shall read data entered by the person requesting access, and if the data is successfully compared to existing data, the portal shall be electrically unlocked. Where required, the system shall provide reasonable assurance that the material surveillance procedure has been met prior to allowing access.
9. Badge readers at MAA shall be equipped with anti-passback protection.
10. Door locks opened by badge readers shall be designed to relock immediately after the door has closed, to deter another person from opening the door without following procedures.
11. Badge reader boxes, control lines, and junction boxes shall be supervised, tamper-alarmed, or equipped with tamper-resistant devices. Multiplexers and other similar equipment shall be tamper-alarmed or otherwise secured.
12. Adequate space shall be designed for exit inspections/searches of all personnel, vehicles, and hand-carried items, including packages, briefcases, and lunch pails to prevent unauthorized removal of SNM. Personnel inspections/searches may be accomplished through the use of SNM portal monitors and metal detectors.
13. Special features (e.g., air locks, enclosed vestibules) shall be considered for access through confinement barriers to minimize the impact of facility access requirements on the ventilation system and to prevent the release of radioactive airborne materials.
14. Provision for normal and emergency equipment access shall be provided in or adjacent to existing ECPs.
15. In designing ECPs consideration shall be given to provision and location of emergency lighting, paging systems, warning and evacuation alarms and lights, and automatic access door switches. If required, space shall be designed for the location of hand and foot monitors, and air sampling and alarm equipment. Additionally, breathing air connections, storage for anti-contamination clothing, and/or change rooms may be required.
16. The location of security inspector posts shall be determined by considering the approved threat level, characteristics of the protected facility, terrain and environment. The security inspector station shall be situated to provide the best available unobstructed view of the surrounding terrain. Posts shall be equipped with duress systems.
17. Stations and electronic equipment where authorization data, badge encoded data, and or personal verification and identification data is input, stored, displayed, or recorded, shall be protected. Protection may be accomplished by continuous surveillance by authorized personnel, structural safeguards, or other means.
18. If keypad devices with scrambled number keypads are not used, the keypad devices shall be installed in such a manner, or have a shielding device mounted, so an unauthorized person in the immediate vicinity cannot observe the selection of keys.
19. Transmission lines that carry access authorization, personal identification, or verification data between devices/equipment shall be protected against the introduction of data that would permit unauthorized access.
20. Metal detectors, special nuclear material monitors, explosives detectors, and x-ray machines, may be used in lieu of or to supplement inspections conducted by protection personnel for prohibited articles and government property (e.g., SNM).
21. When a metal detector is used to inspect personnel entering a Security Area, it shall provide reasonable assurance that weapons are not introduced without authorization.
22. X-ray machines are considered an acceptable means of inspecting bulk and hand-carried items for prohibited articles entering Protected Areas and MAA.

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

24. The use of special nuclear material monitors is an acceptable means of inspecting for concealed special nuclear material.

C. Fencing

1. Fencing shall be limited to that required for safety, physical security, and activity control. In each case the most economical type of fence that will satisfy the particular functional or security requirement shall be selected.

2. Where continuous surveillance over the boundary of the security area is not required, a sturdy, multiple strand or chain-link fabric fence shall serve as the required physical barrier. A more substantial barrier shall be considered for security areas adjacent to heavily populated civilian areas or public highways or where continuous surveillance is required over the boundary of a non-nuclear restricted area.

3. Chain link fabric shall be used to protect security areas designated as limited areas or higher. Fencing shall be at least 8 feet high.

4. Physical protection features shall be implemented at all locations where storm sewers, drainage swells, and site utilities intersect the fence perimeter. Man proofing features shall provide a penetration delay time equal to that required for the security fence.

5. Depressions where water flow is not a problem may be covered by additional fencing suspended from the lower rail of the main fencing.

6. Weed control may justify paving the area beneath fences.

7. A double security fence shall be considered around areas that contain Category I and II special nuclear materials. The Cognizant DOE Operations Office or Operating Contractor's Security and Safeguards Directorate shall be consulted for further design guidance.

8. A clear zone shall be provided along each side of security fence perimeters to facilitate intrusion detection and assessment. Where a double fence is provided, a minimum clear zone of 20 feet shall be considered to the inside and to the outside of the inner and outer fence, respectively. Where minimum distances cannot be provided, supplementary protective measures shall be considered (i.e., greater fence height or other protective measures as required by the cognizant DOE Security Officer). Where feasible, wider clear zone shall be provided. (DOE O 6430.1A, Division 0283)

9. Fences shall be installed not less than 20 feet (6 meters) from the building or material under protection. If the distances specified cannot be accommodated because of property lines, building locations, health and safety, or other site-specific considerations, and unacceptable risk is created, then supplementary protective measures shall be provided.

10. Fencing shall extend to within 2 inches (5 centimeters) of firm ground, or below the surface if the soil is unstable or subject to erosion. Surfaces shall be stabilized in areas where loose sand, shifting soils, or surface waters may cause erosion and thereby assist an intruder in penetrating the area. Where surface stabilization is not possible or is impractical, concrete curbs, sills, or similar types of anchoring devices, extending below ground level, shall be provided.

11. Galvanized steel chain link fabric, consisting of a minimum of 11 gage with mesh openings not larger than 2 inches, shall be used at Security Areas. However chain link fencing is optional for Property Protection Areas. Tension wires or top rail shall be installed along the top edge of the fence fabric.

12. Chain line fencing shall be topped by three or more strands of barbed wire on single or double outriggers. Double outriggers may be topped with coiled barbed wire (or with barbed tape coil where approved for use by the cognizant DOE authority for safeguards and security). When single barbed wire outriggers are used, they shall be angled outward, away from the Security Area.
13. Overall fence height, excluding barbed wire or barbed tape coil topping, shall be a minimum of 7 feet (2.13 meters).
14. Posts, bracing, and other structural members shall be located on the inside of secured perimeters. Once in place, all fence hardware shall be preened or spot welded to prevent easy removal. If the galvanized finish is removed or damaged during installation, the damaged area shall be coated with zinc-enriched paint.
15. Alternative barriers may be used in lieu of fencing if the penetration resistance of the barrier is equal to or greater than standard fencing. Alternative fencing materials:
    - Wood fencing may be used when nonmagnetic requirements are established and to bar vision into limited personnel access areas. However, solid fencing which could increase the need for protective personnel should be used judiciously.
    - Woven wire fencing should be limited to railway and highway rights-of-way.
    - Barbed wire fencing may be used for boundaries of open, undeveloped area.
16. Exterior sensors that serve as the primary means of detection at a security area perimeter shall be designed to assure that a person crossing the perimeter will be detected whether walking, running, jumping, crawling, rolling, or climbing the fence at any point in the detection zone.
17. Refer to the following LANL Master Specification Sections and Standard Details on fences and gates:

    Section 32 3100 Fences and Gates (for stranded fence)
    Section 32 3113 Chain Link Fences and Gates

    ST-G2040-1 Sht 1 Security/Typical Fence
    ST-G2040-1 Sht 2 Pedestrian Gate
    ST-G2040-1 Sht 3 Double Leaf Vehicle Gate
    ST-G2040-1 Sht 4 Gate Latching
    ST-G2040-1 Sht 5 Hill Side Fence
    ST-G2040-1 Sht 6 Embankment Fence
    ST-G2040-1 Sht 7 Top of Embankment Fence
    ST-G2040-1 Sht 8 Bottom of Embankment Fence
    ST-G2040-1 Sht 9 Fence Manproofing

D. Security Gates

1. Motorized gates shall be considered for primary access points. Motorized gate controls shall be located within guard stations at each access point. Motorized gates shall be designed to allow manual operation during power outages.
2. Electrical continuity shall be provided across all gate openings. Operating mechanisms for motorized gates shall be grounded in a similar manner.
3. Points of vehicle and pedestrian access to restricted areas shall provide the same level of physical protection as that provided at all other points along the secured perimeter. Gate hardware for security fencing shall be installed in a manner that will prevent or mitigate tampering.
4. Gate hardware for security fencing shall be installed in a manner to mitigate tampering and/or removal (e.g., brazed, peened, or welded).

E. Walls

1. Walls serving as security area boundaries shall meet the following requirements:
2. Building materials shall offer penetration resistance to, and evidence of, unauthorized entry into the area. Construction shall meet local building codes.
3. When transparent glazing material is used, visual access to the classified material shall be prevented by the use of drapes, blinds, or other means.
4. Panel type exterior finish systems, if used, shall be installed such they cannot be removed from outside the area being protected without showing visual evidence of tampering.
5. Walls that constitute exterior barriers of Security Areas shall extend from the floor to the structural ceiling, unless equivalent means are used.
6. Walls defining an MAA boundary shall be designed or constructed so that penetration within the specified delay times is not credible. Some type of monitoring shall be provided where penetration is credible. Designs in which the walls are easily penetrated are not advisable. MAA walls shall not provide hiding places or redoubt-like structures for adversaries.

F. Ceilings and Floors

1. Ceilings and floors shall be constructed of building materials that offer penetration resistance to, and evidence of, unauthorized entry into the area. Construction shall meet local building codes.

G. Security Doors

1. Doors that serve as exits from security areas shall comply with NFPA 101, Chapter 4, and with DOE security requirements, except the use of panic hardware on doors from security areas shall be limited to assembly and hazardous occupancy classifications of the Code as determined by the DOE cognizant authority.
2. Where primary reliance is placed on doors as physical security barriers, they shall provide a penetration resistance equal to that specified in the site-specific security plan for adjoining walls, ceilings, and floors.
3. Where more than one door is required for emergency egress from a security area, single doors or double doors with a removable mullion between them shall be used.
4. Doors that serve exclusively as exits from security area shall not be operable from outside the security area.
5. Doors that serve as emergency exits from spaces should not open into spaces of greater security.
6. Doors with transparent glazing material may be used if visual access is not a security concern; however, they shall offer penetration resistance to, and evidence of, unauthorized entry into the area.
7. A sight baffle shall be used if visual access is a factor.
8. Openings in doors shall be covered to provide the necessary barrier delay rating required by the site-specific security plan for that door. Various materials and configurations may be used, if they are approved by the cognizant DOE safeguards and security authority.
9. An astragal shall be used where doors used in pairs meet.
10. Door louvers, baffle plates, or astragals, when used, shall be reinforced and immovable from outside the area being protected.

11. Where used to enhance penetration resistance, wire mesh shall be 2-inch square or smaller mesh of No. 11 American Wire Gauge or heavier steel wire or expanded metal.
12. Doors of offices or rooms constituting security area perimeters where Secret or Top Secret information is discussed on a recurring or routine basis shall be constructed of materials of low sound conductivity, or shall otherwise be soundproofed in accordance with DOE M 470.4-4 Section E, Chapter IV and the DOE Technical Surveillance Countermeasures (TSCM) Procedural Guide so as to prevent a person outside the room with reasonable access to the wall from overhearing a conversation at normal voice level within the room without the use of hearing instruments or equipment.
13. Access doors to security posts shall be provided with positive locking devices to prevent unauthorized entry.
14. The design of MAA exit doors, vault doors, vault racks, containers, etc., should provide for seal Tamper Indicating Devices (TIDs) mechanisms. Requirements for TIDs are contained in DOE M 470.4-2. DOE/EP/0035 should also be considered.
15. Personnel access to various parts of a facility and/or materials within the facility may need to be controlled at a finer level than that provided by the security boundary. To accomplish this, it may necessary to subdivide the security area into rooms or sets of rooms to which access is granted by electronic card systems, keypads, guard stations, or other devices. This reduces the number of people having access to a wide range of materials or classified matter.
16. For a vault containing SNM, a type of door and frame complying with GSA-approved Class 5 vault doors shall be the required level of physical protection.

H. Hardware

Screws, nuts, bolts, hasps, clamps, bars, wire mesh, hinges, and hinge pins shall be fastened securely to preclude removal and to ensure visual evidence of tampering. Hardware accessible from outside the area shall be peened, brazed, or spot-welded to preclude removal, or otherwise be secured by hardware that is resistant to tampering (e.g., non-removable hinge pins).

I. Locks

1. Locks used in the protection of classified matter and Categories I and II special nuclear material (e.g., security containers, safes, vaults) shall meet Federal Specification FF-L-2740 "*Locks, Combination*."
2. Combination padlocks shall meet Federal Specification FF-P-110, "Padlock, Changeable Combination," and standards cited in 41CFR101 "*Federal Property Management Regulations*."
3. High-security, shrouded-shackle, key-operated padlocks shall meet the standards in Military Specification MIL-P-43607, "*Padlock, Key operated, High Security, Shrouded Shackle*," or its successor. High-security key padlocks are approved to secure Category I and II special nuclear material and Top Secret Matter.
4. Key locksets shall meet ANSI Standard A156.2, "*American National Standards for Bored and Pre-assembled Locks and Latches*."
5. Lock bars shall be 1-1/4 inch (31.75 mm) by 3/16 inch (4.76 mm) or equivalent in cross section and constructed of material hardened to Rockwell C59 to C63 standards.
6. Hasps and yokes on repositories containing classified matter shall be constructed of material hardened to Rockwell C59 to C63 standards; be at least 1/4 inch (6.35 mm) in diameter, or equivalent cross section; and be secured to the repository by welding or riveting.

7. Panic hardware or emergency exit mechanisms used on emergency doors located in Security Areas shall be operable only from inside the perimeter and shall meet NFPA 101, the Life Safety Code.
8. Locks used in the protection of classified matter and Categories I and II special nuclear material (e.g., security containers, safes, vaults) shall meet Federal Specification FF-L-2740 "*Locks, Combination*." This is applicable to locks purchased or installed after the date of this chapter and for replacement of damaged equipment.
9. High-security, shrouded-shackle, key-operated padlocks shall meet the standards in Military Specification MIL-P-43607, "*Padlock, Key operated, High Security, Shrouded Shackle*." High-security key padlocks are approved to secure Category I and II special nuclear material and Top Secret Matter.

J. Windows

1. Where primary reliance is placed on windows as physical security barriers, they shall provide a penetration resistance equal to that specified in the site-specific security plan for adjoining walls, ceilings, and floors. Such windows shall be constructed of shatter-resistant, laminated glass panes of 9/32-inch minimum thickness or other material providing an equal degree of resistance, and installed in fixed (e.g., inoperable) frames so that the panes are not removable from outside the area being protected.
2. Window frames must be securely anchored in the walls, and windows should lock from the inside. Swing-out steel sash (industrial-type) frames are acceptable for window installation provided the windows can be securely locked or are permanently sealed shut.
3. Where used to increase penetration resistance, wire mesh shall be 2-inch square or smaller mesh of No. 11 American Wire Gauge (AWG) or heavier steel wire or expanded metal.
4. Visual barriers shall be used if visual access is a factor.

K. Unattended Openings

1. Physical protection features shall be implemented at all locations where storm sewers, drainage swells, and Site Utilities intersect the fence perimeter.
2. Unattended openings in security barriers must incorporate manproofing measures such as security bars if their size and location is:
    - Greater than 96 inches square (619.20 square centimeters) in area and greater than 6 inches (15.24 centimeters) in the smallest dimension.
    - If it is located in a wall or other structure constituting the Security perimeter and it is located within 18 feet (5.48 meters) of the ground or roof, or any architectural feature that might provide access such as a ledge or fire escape.
    - Located 14 feet (4.26 meters) diagonally or directly opposite windows, fire escapes, roofs, or other openings in uncontrolled adjacent buildings; or
    - Located 6 feet (1.83 meters from any other uncontrolled opening in the same barrier.
3. The rigid metal bars used for man proofing shall be securely fastened at both ends to preclude removal.
4. Where wire mesh, expanded metal, or rigid metal bars are used, care shall be exercised to provide reasonable assurance that classified matter within the vault cannot be removed with the aid of any type of instrument.

5. During construction, any annular space around any duct, pipe or conduit which penetrates a security perimeter wall and is not otherwise sealed for fire proofing, shall be covered by an escutcheon or filled with lead, wood, waterproof caulking, or similar material, to give evidence of tampering or surreptitious removal.
6. For man-proofing ductwork, refer to the following LANL Standard Details:
   ST-D3040-6 (1of 2) Typical HVAC Duct Security Bars
   ST-D3040-6 (2 of 2) Typical HVAC Duct Security Bars

L. Entry Portals

1. Nuclear material shall be transferred into and out of the MAA at well-defined locations (usually loading docks) subject to specific procedures and monitoring that prevent unauthorized transfers.
2. Portal systems in MAA boundary areas shall allow for the passage of personnel while detecting the presence of nuclear material and metal. Sometimes, in addition, equipment/package portals are used so that tools and packages can be monitored separately. The following should apply to the design of portals:
3. Special nuclear material portal monitors should be distanced from or shielded from nuclear materials in the process area. This applies not only to locations of static storage, but to passageways or conveyer systems that allow the passage of materials within the facility.
4. Portal monitors shall be located so that it is not physically possible to pass items around the portal without those objects' undergoing some sort of surveillance (e.g., passing through the guard station).
5. Portal monitors are generally co-located with guard stations, so that an adequate response to an alarm is available. The guard station should be provided with an unobstructed view of the portal monitor. Unattended portals require careful design to assure response to and resolution of alarms.
6. In processing areas, provisions shall be made for planned and emergency evacuations. Where this evacuation occurs through the MAA boundary, alarmed doors shall be provided, as it is generally not feasible or cost effective to use unmanned portal monitors at all required exits.
7. In the case where emergency exits are not monitored, provision shall be made to assure that evacuations do not provide a theft opportunity. Emergency exits can exit into a secured outer area within a security fence which provides an evacuation or shelter area with sufficient physical separation from the structure or a pathway to such an area. Local administrative procedures can then require that the evacuation or shelter area is placed under surveillance by the protective force during any evacuation and swept with SNM detectors afterward to make sure no material has been left behind.
8. Effective use of the SNM detectors requires that the monitored areas not be too large and that they have low background radiation levels. Accordingly, SNM portal monitors should be distanced from or shielded from nuclear materials in the process area. This applies not only to locations of static storage, but to passageways or conveyer systems that allow the passage of materials within the facility.
9. Bypass routes around portal metal detectors and/or special nuclear material monitors, as applicable, shall be closed or monitored to deter unauthorized passage of personnel and hand-carried articles.
10. Measures shall be taken to preclude the unauthorized changing of control settings on portal monitoring equipment.

M. Vehicle Barriers

1. Speed reducers shall be considered for use at entry control points to slow approaching adversary vehicles to within vehicle barrier design limits if needed to achieve site-specific threat/target system response requirements consistent with the operational and protection goals of the facility.
2. The installation of vehicle barriers (e.g. Jersey barriers) inside or outside a perimeter fence shall be considered where the secured perimeter borders public vehicular traffic areas or where a high speed approach may be attempted to breach the perimeter fence. Wire-rope-type vehicle barriers may also be considered for this purpose.
3. If above grade vehicles barriers are used outside on any security perimeter, consideration shall be given in the design of the barriers to not create any areas of concealment or redoubt like structures which might be used in a malevolent attack on the facility.
4. In additions to barriers, entry and access portals shall provide equivalent delay to vehicles and personnel. For most protected-area perimeters, electrically operated fence gates shall be considered. Protection shall be provided against vehicle ramming. Techniques used to fulfill these requirements include speed reducing curves, hydraulic bollards, specially designed gates and vehicle traps, and steel cables attached to perimeter fence posts.

N. X-ray Units

1. If used, X-ray machines shall be capable of imaging a 26-gauge wire at Step 5 on an ASTM step wedge (ASTM 792).
2. Compensatory measures shall be available at each location to provide equal detection probabilities in the event of X-ray machine failure.
3. Appropriate shielding and protection against chronic health effects from use of the X-ray equipment shall be provided for the operators.

5.4 Lighting and Electrical Power Requirements

A. Standard Security Lighting

1. Adequate protective illumination shall be provided to detect adversaries, reveal unauthorized persons, and, at pedestrian and vehicular entrances, to allow examination of credentials and vehicles.[3]
2. Protective lighting, as part of a security system, should be used as needed for proper physical protection of attractive materials and/or classified matter.
3. Where required, lighting systems shall have a backup electrical power system to minimize the interruption of illumination in case of a loss of site power.
4. Protective lighting in Protected Areas, Material Access Areas, and Vital Areas shall be adequate to provide 24-hour visual assessment.
5. Lighting installed at security posts shall be capable of providing a minimum illumination of 2 foot-candles at ground level for at least a 30-foot-diameter circle around the security inspector post and 0.2 foot-candle for 150 feet in all directions.

[3] Chapter 7 in DOE M 5632.1C-1, *Manual for Protection and Control of Safeguards and Security Interests* for this and several other requirements in this subsection.

6. Light glare shall be kept to a minimum in situations where it would impede effective operations of protective personnel; interfere with road traffic; or be objectionable to occupants of adjacent properties. Make every attempt to comply with the New Mexico Night Sky Protection Act through careful selection/spacing of fixtures; non-compliant designs require approval by both the ESM Security and Electrical POCs.
7. Light sources on protected perimeters shall be located so that illumination is directed outward, wherever possible.[4]
8. Lamps in which light is produced directly or indirectly by the use of gas, such as sodium vapor and other high intensity discharge (HID) lamps, are highly efficient and economical in operation, and their use in protective lighting systems is encouraged. However, it should be recognized that gas lights require a relight period of approximately 3 minutes following any power interruption.
9. Where HID lamps are used and where continuous lighting is required, a standby lighting system shall be considered to ensure the maintenance of minimum protective lighting during HID lamp start-up and re-strike periods. Fixtures adjacent to each other shall when practical and appropriate be placed on different circuits so that only a portion of the lighting is extinguished if one circuit becomes inoperative.[5]
10. For facilities requiring protective lighting, consideration shall be given to having an emergency lighting capability of the type and size required in relation to the importance of the facility, reliability of regular power sources, and feasibility of using portable lighting equipment.
11. Where protective lighting at remote perimeters is not feasible, protective force patrols and freed stations maybe equipped with night vision devices, although it should be recognized that adequate perimeter lighting provides better protection and deterrence to intrusion than do night vision devices. Night vision devices shall not be used in lieu of protective lighting at ingress and egress points.
12. Adequate light levels are necessary to ensure optimum performance in all work areas. Glare and shadowing shall be avoided. For recommended control room illumination levels, luminance ratios, reflectance levels and further lighting considerations, see DOE O 6430.1A, Section 1655 Interior Lighting; and NUREG 0700, Section 12.1.2.3. Lighting design shall consider environmental degradation effects (such as dust or radiation on viewing ports) to ensure adequate lighting intensities can be provided on a long-term basis.
13. Design security lighting systems in accordance with Chapter 29 in the IESNA *Lighting Handbook.*

B. Emergency Lighting Requirements

Emergency lighting systems shall be provided as required by NFPA 101. A control room emergency lighting system shall be automatically activated and immediately available for a stated minimum length of time on failure of the normal lighting system. The emergency lighting system for vital areas shall be an electrically independent system that is not degraded by failure of the normal lighting system. Control room emergency lighting levels shall be in accordance with NUREG 0700, Section 12.1.2.4.

C. Power Supply Protection Requirements

1. Primary power for protective alarm and communications systems shall normally come directly from the on-site power distribution system. In the case of isolated facilities, power may come directly from the public utility. Where several primary power sources are available, the most reliable source shall be used.

[4] Chapter 7 in DOE M 5632.1C-1, *Manual for Protection and Control of Safeguards and Security Interests.*
[5] Refer to the Lighting Equipment heading Chapter 29 in the *IESNA Lighting Handbook*, ninth edition

2. Definition of "emergency systems," "legally required standby systems," and "optional standby systems" shall be in accordance with NFPA 70, the National Electrical Code (NEC).
3. Emergency power systems legally required by NFPA 70 shall be installed to meet normal emergency power requirements. More stringent emergency power requirements may be identified by the DOE cognizant authority on a case-by-case basis.
4. Primary and Emergency or Standby power source which comply with Section 1640-3.3 of DOE O 6430.1A shall be provided for the following security systems and/or functions.
    - Security Communications systems.
    - Intrusion detection systems for protection of Categories I and II special nuclear material, Vital Equipment, and Top Secret matter.
    - Entry Control Point (ECP) operations and communication systems.
    - Other components whose operating continuity is determined to be vital by the cognizant DOE authorities for protection of health, life, property, and safeguards and security systems.
5. Safety Class 1 items (or current equivalent) shall be provided with emergency power.
6. For those security areas requiring Emergency or Standby power, transfer to the auxiliary power source shall be automatic upon failure of the primary source and shall have no effect on operation of the security system or device. Loss of primary power and actuation of Emergency/Standby power shall be indicated on an annunciator panel. The annunciator shall be located in an occupied area and shall indicate any problems with the emergency system. If applicable, the central alarm station shall receive an alarm indicating failure of the security system power and transfer to the auxiliary power source. In the case of Category I and II quantities of special nuclear material Protection Areas and Vital Equipment, both the Central Alarm Station and Secondary Alarm Station shall receive the alarm.
7. Emergency and standby power systems shall be design to serve the loads set forth in NFPA 110.
8. Emergency power systems shall be capable of maintaining full operation of emergency loads for the full time period specified by the DOE cognizant authority (nominally, a minimum of 24 hours).
9. Where emergency or standby generators are required for loads 25 kVA and smaller, gasoline or liquefied petroleum gas (LPG) engines may be used. For loads greater than 25 kVA, diesel engines shall generally be used. Steam-turbine generators may be used if steam is being produced for on-site processes. Gas turbines may be used if a life-cycle cost (LCC) analysis warrants and if the NEC criteria to emergency power throw-over time is met.
10. Where possible, control and test panels for required Emergency or Standby power systems should be located within a Protected Area. In not within a protected area, Emergency or Standby power system components such as test panels, starter panels, sensors, junction boxes, etc. shall be tamper-resistant or tamper-alarmed.
11. Emergency power equipment areas shall be ventilated to exhaust hazardous gases (if applicable) and to maintain satisfactory ambient temperatures for equipment operation or personnel access.
12. An uninterruptible power systems (UPS) shall be considered for loads that, if interrupted, would degrade the security of the associated area. The UPS system shall comply with DOE O 6430.1A, Section 1660-3, Uninterruptible Power Systems and Underwriters Laboratory (UL) 752. NIJ Standard 0108.01 should be considered for facilities housing UPS systems.
13. Uninterruptible power supplies shall be provided for those loads requiring guaranteed continuous power. Application of UPSs shall comply with IEEE 446, as modified by the DOE cognizant authority. UPS installations shall be designated as Safety Class 1 (Seismic Category I functional) or standby type dependent on the classification of the loads served.

14. Batteries, when required, shall be rechargeable and shall be kept fully charged at all times when primary power is available. The charger shall automatically switch from float to fast charge rate at a preset drop in DC bus voltage. The charger shall be furnished with a capacity to charge the battery from a fully discharged state to not less than 85 percent of the rated ampere-hour capacity within 24 to 72 hours. See also IEEE 308.
15. Required emergency and standby power sources shall have the necessary built-in features to facilitate operational testing on a periodic basis to verify their readiness.
16. Refer to ESM Chapter 7 for addition requirements and guidance on backup power sources (e.g., Section D5090).

5.5 Interior Intrusion Detection and Automated Access Control Subsystems (IIDS/AACS or IDS/ACS)

A. Introduction

1. The intrusion detection system (IDS) and access control system (ACS) described herein shall follow the design specifications herein to provide an overall electrical infrastructure necessary to meet the requirements delineated in the Orders and Manuals. LANL's Security Systems Group (PS-2) maintains final design approval authority of all Laboratory IDS & ACS installations and must be engaged from the onset of all security system design activities.
2. Design of this system, as described in this section shall be based on the DBT and current orders and manuals as augmented by the LANL Security Systems Group unless otherwise directed and formally documented by LANL's Classified Matter Protection (PS-1) group.[6] LANL's Security Systems Group (PS-2) will complete the installation of the IDS & ACS security system in accordance with DOE Order 470.4, DOE M 470.4-2, DOE M 470.4-4, and DOE M 470.4-2 Section B. Where there is room for interpretation of the Manual or Orders, PS-2 will pursue a conservative approach in our application of protection strategies. These strategies have been consistently validated by DOE's Office of Assessment.
3. Intrusion Detection Systems (IDS) and Access Control Systems (ACS) will include one or more of the following sub-systems and will be coordinated with project-specific requirements with the LANL Security Systems Group (PS-2).

a. General Components
- LANL Field Panel (LFP).
- Argus Field Processor (AFP)
- Copper and fiber optic cables (data and control).

b. Access Control Systems (ACS)
- Door access control systems with badge readers, biometric units, and door hardware (strikes or latches) with key overrides.
- Turnstile access control systems with badge readers and/or biometric units. Turnstile egress may be accomplished with a push button or badge reader.

c. Intrusion Detection Systems (IDS)
- Volumetric, perimeter, and/or point contact detectors

[6] Physical security system design is a graded process. It includes determining the objectives, designing the system with inherent detection, delay and response constituents, and then evaluating the design with regards to meeting the objectives. Physical constituents of an adequate design include fencing, gates, barriers, grading, drainage, and roads, lighting, security barrier penetrations, such as utility and sound barriers, CCTV systems, intrusion detection systems, and entry control points. Special nuclear material protection has further design requirements.

- Door sensor switches
- CCTV

4. Coordinate IDS and ACS design and installation requirements with the LANL Classified Matter Protection Group (PS-1). PS-1 will assign a Security representative to facilitate activities between the Project and the LANL Security Integration Group (SO-3), the LANL Security Systems Group (PS-2), and PS-1. LANL's security system activities will be integrated with the project.
    - For new facilities, the IDS/ACS objectives will be defined and the PSS designed and evaluated.
    - For existing facilities, the IDS/ACS objectives will be re-examined to ensure adequacy and then the IDS/ACS designed and evaluated.
    - In all cases, performance testing will be accomplished prior to final acceptance and certification.
5. GFE: Security system control electronics to include biometric units, badge readers, door sensor switches, volumetric detectors, and CCTV equipment will be furnished and installed by the LANL Security Systems Group (PS-2). Contractor will install all electrical infrastructures (conduit, cable, boxes, fittings, etc) per Project drawings bearing approval from LANL's Security Systems Group's Design Team.
6. LANL PM Planning: Include in the project budget sufficient funding for LANL-furnished security system materials, labor, and equipment. Include in the project schedule and budget sufficient time and funding for the installation of security system devices and performance testing by the LANL Security Systems Group. Obtain a cost estimate and schedule from LANL Security Systems Group.
7. Coordination: The installation of security system devices will begin after beneficial occupancy. Contact LANL Security Systems Group (PS-2) for exceptions.
8. Testing: DOE/NNSA-mandated performance testing will begin after the installation of field devices is completed. Prior to all LANL security system certifications, PS-2 will conduct formal Performance Testing activities pursuant to the aforementioned DOE Manual and Orders.

B. Pathways for IDS/ACS

1. Install security system wiring in conduit system. Coordinate design of the conduit system with the LANL Security Systems Group.
2. Select conduit sizes on the following basis:
    - Less than 50 feet between pulling points and only one bend: 40 percent fill.
    - More than 50 feet between pulling points or two 90-degree bends: 31 percent fill.
    - Minimum size: 1 inch unless specified otherwise.
3. Coordinate locations of all IDS/ACS outlet boxes and enclosures with the LANL Security Systems Group. Coordinate locations of all IDS/ACS boxes with the LANL Security Systems Group. *This coordination will result in a signed document verifying the number and location of each box.* LANL will furnish specialty boxes as GFE, typically:
    - 10" x 10" x 4" junction boxes.
    - 60" wide x 60" high x 12" deep Laboratory Field Panel (LFP) enclosures, or a 36" wide x 36" high x 12" deep Laboratory Field Panel (LFP) enclosures.
    - 4" x 4" x 4" Access/Secure switch and pushbutton boxes.
    - Badge reader and biometric unit mounting brackets.
4. The LANL Security Systems Group will furnish as GFE the copper and fiber optic cables for data and control for IDS/ACS field devices.

5. The LANL Security Systems Group will perform all terminations of data and control cables.
6. Use materials and installation methods described in LANL Master Specification Section 25 0533, *Raceways and Boxes for Electrical Systems.*
7. Labeling will be performed by LANL; device acronyms are per ESM Ch. 1 Section 230.

C. Security Service Entrance

1. For security systems not protecting Category I or II SNM provide one security service entrance pathway from the point of connection to the telecommunications network (manhole, pedestal, etc.) into the entrance telecommunications room. The pathway may use the telecommunications service pathway to the building.
2. For security systems protecting Category I or II SNM provide two separate security service entrance pathways from the point of connection to the telecommunications network (manhole, pedestal, etc.) into the entrance telecommunications room.[7]
   - One or both of the pathways may use the telecommunications service pathway to the building if the physical separation requirement is met.
   - The security service entrance pathways must have a wall-to-wall separation of not less than 16 inches to reduce the possibility of simultaneous disruption
   - Minimum pathway is 2-inch conduit.
3. Use materials and installation methods described in LANL Master Specification Section 33 7119, *Electrical Underground Ducts and Manholes*.
4. LANL's Telecommunications Group will furnish, install, and terminate the security service entrance cables.
5. Refer to the following Standard Details (draft, if available):

   Security Systems General Infrastructure Installation Requirements:

ST-F1033-1	AFP, BAT, FTB, and GUT Elevation and Mounting Details
ST-F1033-2	Laboratory Field Panel Details
ST-F1033-3	Security Area Access – Controlled Entrance Door
ST-F1033-4	Security Area Infrastructure – Elevations and Details
ST-F1033-5	Sensor Termination Box Mounting Details
ST-F1033-6	Security Door: Electric Strike and Electric Latch Details
ST-F1033-7	RAP and HGU Elevation and Mounting Details
ST-F1033-8	Volumetric Infrastructure: High and Low Bay Arrangements
ST-F1033-9	Cable Routing Requirements

5.6 Communication and Cyber Security -- Protected Transmission Systems (PTS)

A. General

1. Design protected transmission systems (PTSs) as described in this section as required to meet the users' secure communications needs in LANL facilities.
2. Conform to the requirements of the latest editions of (and amendments to) the TIA/EIA standards referenced for unclassified telecommunications systems[8], the NEC, DOE M 200.1-1—

[7] Refer to Chapter 7 in DOE M 5632.1.C-1. Defense in depth for Category I and II SNM requires redundant, independently routed communications paths to avoid a single-point failure.

Telecommunications Security Manual, the LANL PTS Master Plan, and this chapter of the LANL Engineering Standards Manual. (The use of the "For Official Use Only" document DOE M 200.1-1 and the PTS Master Plan will be coordinated through the LANL PTS Site Manager.)

3. Coordinate PTS design requirements with the LANL PTS Site Manager and the LANL Telecommunications Group.
4. Before beginning PTS construction obtain approval of the design drawings and the "Protected Transmission Systems CDIN/PTS Security Plan Request for Access to a Secure Communications Utility" from the LANL PTS Site Manager.
    a. The construction contractor shall furnish and install the PTS pathway system.
    b. LANL will perform a technical inspection of the contractor-installed PTS pathway system.
    c. LANL will furnish the terminal connection boxes for construction contractor installation.
    d. LANL will furnish and install the PTS patch panels and terminal connection devices.
    e. LANL will install PTS cables and connectors then will terminate and test all PTS cables.
5. After construction of the PTS, detailed "as-built" drawings showing outlets, routing of pathways, junction boxes and pull boxes must be submitted to the LANL PTS Site Manager prior to activation approval.
6. Include in the project budget sufficient funding for LANL-furnished PTS material, labor, and equipment. Include in the project schedule and budget sufficient time and funding for the inspection of PTS pathways, installation of PTS outlets and electronics, performance testing, and field quality assurance activities by LANL. Obtain a definitive cost estimate and schedule from the LANL Telecommunications Group and the LANL PTS Site Manager.
7. Refer to LANL Master Specification Section 27 1500.18, *Protected Transmission System Rough-In*, for PTS material and installation requirements.

B. Definitions[9]

CDIN: The abbreviation for "classified distributive information network" that is any cable, wire, or other approved transmission media used for the clear text transmission of classified information in certain DOE controlled access environments. Excluded is any system used solely for the clear text transmission and reception of intrusion/fire alarms or control signaling.

CDIN-1: A type of CDIN used in a Limited Area.

CDIN-2: A type of CDIN used in a Property Protection Area.

RED: Designation applied to information systems and associated areas, circuits, components and equipment in which National Security Information (classified) is processed. (BLACK is the designation applied to information systems and associated areas, circuits, components and equipment in which National Security Information is not processed (unclassified). Encrypted signals are unclassified.)

Terminal Connection: A term used at LANL to refer to the point where the user connects to the secure communications utility (personal computer interface). Terminal connections are commonly referred to as "drops." The connection is also often referred to as a Protected Outlet Box (POB).

---

[8] TIA and EIA telecommunications standards are useful because PTS systems are fundamentally telecommunications systems.

[9] Definitions from *Telecommunications Security Manual* as adopted for LANL use in the "Los Alamos National Laboratory Protected Transmission System (PTS) Master Plan" dated March 1, 2004.

C. PTS Topology

1. In large facilities (larger than 25,000-sq. ft.) design a system of dedicated secure (RED) telecommunications rooms for terminating PTS entrance pathways, PTS backbone pathways, and PTS horizontal pathways. Provide secure (RED) server rooms that are connected to the RED telecommunications rooms by PTS backbone pathways.
2. In a smaller facilities use the RED server room as the termination point for PTS entrance pathways and PTS horizontal pathways.

D. RED Telecommunications Rooms

1. Design dedicated RED telecommunications room(s) that meet relevant requirements described for unclassified telecommunications rooms in ESM Chapter 7 Section D5030 (for addressing architectural, HVAC, electrical power, lighting, grounding, and determination of need for temperature monitoring equipment with remote signaling capability), plus the following additional requirements:
   a. Provide RED telecommunications room(s) in addition to the unclassified telecommunications room(s). If possible, locate the RED telecommunications room(s) adjacent to the unclassified telecommunications room(s).
   b. Locate RED telecommunications room(s) in the secure part(s) of the building.
   c. Increase the size of the RED telecommunication room(s) to accommodate one or more RED patch panel racks (each a minimum of 29" wide by 34" deep) and to provide not less than the required RED/BLACK separation from BLACK equipment, signal/data lines, power lines, and "fortuitous conductors." RED/BLACK separation requirements depend upon the PTS transmission media. Obtain RED/BLACK separation requirements from the LANL PTS Site Manager.

E. RED Server Equipment Room(s)

1. Design dedicated, RED server equipment room(s) as required to meet the Users' programmatic needs. *RED server rooms are often designated as "vault-type rooms" having special security system requirements—refer to Electronic PSS section above*. Based on determination of programmatic needs requiring the RED server rooms to house large numbers of computers, servers, and other electronic equipment that is capable of reaching high temperature limits, refer to ESM Chapter 7 Section D5030 for determination of need and design guidance for temperature sensors, thermostats, and related components. This section provides the appropriate guidance on HVAC load density. The load is to be used as a first approximation for RED server rooms housing server equipment, computers, or other electronic equipment capable of increasing the heat loading with in the area. HVAC requirements must be coordinated with the server equipment owner.
2. Design RED server room(s) to meet requirements for unclassified telecommunications server rooms plus the following additional requirements:
   a. Locate RED server room(s) within the secure part(s) of the building.
   b. Locate RED server rooms adjacent to RED telecommunications rooms (if used).
   c. Provide not less than the required RED/BLACK separation from BLACK equipment, signal/data lines, power lines, and "fortuitous conductors." RED/BLACK separation requirements depend upon the PTS transmission media. Obtain RED/BLACK separation requirements from the LANL PTS Site Manager.

F. PTS Terminal Connections

1. Each PTS terminal connection will consist of a LANL-furnished surface-mounted box with LANL-furnished and installed fiber-optic cables and connectors.

2. Position each PTS terminal connection at a readily accessible location 42 inches above the floor. *PTS terminal connection should be located at least 30 inches from corner of room to prevent being blocked by furnishings. Visual access prevention must be considered when locating the PTS terminal connection.*

G. PTS Horizontal Pathways

1. Design PTS horizontal pathway systems to meet applicable requirements in EIA/TIA-569-A, the NEC, DOE M 200.1-1, the LANL PTS Master Plan, and this Chapter.
2. In Limited Areas provide PTS horizontal pathways as follows: [10]
   a. Exposed: CDIN-1.
   b. Above easily accessible ceilings or below an easily accessible floor: CDIN-1. *Note that an unexposed CDIN must receive visual and technical inspections more frequently than an exposed CDIN. The User should evaluate this stream of future costs compared to the aesthetic benefits of concealing the CDIN.* Approval for unexposed CDIN must be obtained on a case-by-case basis from the LANL PTS Site Manager.
3. In Property Protection Areas design PTS horizontal pathways as follows: CDIN-2.
4. PTS pathways shall not be installed in the public domain (Uncontrolled Access Areas) at LANL.[11]
5. Physical requirements for CDIN-1 pathways are as follows:
   a. Use conduits, wireways, and boxes made of ferrous material; use Intermediate Metal Conduit (IMC)
   b. Secure covers for boxes with tamper-resistant fasteners. Secure wireway covers with tamper-resistant fasteners.[12]
   c. Position pathways with respect to mechanical equipment, ductwork, piping, and fixed architectural finishes so the pathways will be continuously inspectable.
   d. Maintain a 2 inch RED/BLACK separation throughout the CDIN pathways. Obtain RED/BLACK pathway separation requirements from the LANL PTS Site Manager.
6. CDIN-2 pathways must meet CDIN-1 requirements plus all joints, connections, cracks, seams, doors, etc. must be sealed with a properly administered tamper-indicating seal approved by DOE. *Welding or conductive epoxy may also be used at the discretion of the cognizant DOE office.*
7. PTS pathways must pass a comprehensive technical inspection by the LANL PTS Site Manager.
8. Use NRTL-listed metal wireways to distribute multiple PTS cables from RED patch panel racks to the vicinity of the PTS terminal connections. Wireway systems shall meet the appropriate CDIN requirements and the following criteria:
   a. Size raceway based on one cable per terminal connection.[13]
   b. Cable outside diameter approximately 0.25".
   c. Provide for 20% future growth in the number of PTS cables.
   d. Initial wireway fill shall not exceed the following values:

---

[10] Refer to Chapter 5 in DOE M 200.1-1.
[11] "Los Alamos National Laboratory Protected Transmission System (PTS) Master Plan" dated March 1, 2004.
[12] Tamper-resistant fasteners required by the "Los Alamos National Laboratory Protected Transmission System (PTS) Master Plan" dated March 1, 2004.
[13] Typical configuration is called "KVM"; the user's computer is in the RED server room and is connected via the PTS to a keyboard, video display, and mouse at the terminal connection in the workspace.

- 41.7% of the wireway cross-sectional area if there are no current-carrying electrical conductors in the wireway.[14]
- 16.7% of the wireway cross-sectional area if there is any current-carrying electrical conductor in the wireway.[15]

e. Locate PTS wireways or conduits 3 inches above ceiling tiles with sufficient space to permit access for installing and maintaining cables and for security inspections. *Careful design and installation coordination with the building structure, HVAC ductwork, sprinkler piping, and luminaires is required to maintain the required access. Develop "plan and profile" type drawings for each PTS wireway to assure meeting this requirement.*

f. Refer to Section 27 1500.18, *Protected Transmission System Rough-In,* for wireway material and installation requirements.

9. Provide an individual 1-inch IMC from PTS wireway to each PTS terminal connection. Design conduit systems to meet the appropriate CDIN requirements. Refer to Section 27 1500.18, *Protected Transmission System Rough-In,* for conduit material and installation requirements.

H. PTS Backbone and Entrance Pathways

1. For large buildings provide the following secure backbone and entrance pathways:

   a. Provide a minimum of two 4-inch CDIN conduits interconnecting secure patch panel racks in the vertically aligned secure telecommunications rooms in a building.[16]

   b. Provide a minimum of one 4-inch CDIN conduit interconnecting secure equipment racks in multiple secure telecommunications rooms or secure server rooms on a floor.[17]

   c. Provide an underground ductbank with a minimum of two 4-inch ducts from the point of connection to the network (telephone manhole or telephone pedestal as directed by LANL Telecommunications Group) into the entrance secure telecommunications closet.[18] Terminate PTS entrance conduits in a 24" x 24" x 12" hinged-cover box.

2. For small buildings install an underground ductbank with a minimum of two 4-inch ducts from the point of connection to the network (telephone manhole or telephone pedestal as directed by LANL Telecommunications Group) into secure server equipment room.[19] Terminate the conduits in the secure equipment rack.

3. Maintain not less than 6 inches separation between PTS entrance conduits and any other utility. Encase conduits for SRD systems in concrete providing not less than 3 inches coverage on all sides. Encase conduits for TSRD systems in concrete providing not less than 8 inches coverage on all sides. Place the top of the ductbank not less than 3 feet below finished grade.[20] Identify the PTS entrance conduits with red spray paint placed 3-ft on centers.

4. Use materials and installation methods described in LANL Master Specification Section 26 0533, *Raceways and Boxes for Electrical Systems* and Section 33 7119, *Electrical Underground Ducts and Manholes*.

---

[14] NEC Section 770.12 removes raceway fill limitations if there are no current-carrying conductors; however, clause 4.5.3 in TIA/EIA-569-A sets an absolute maximum wireway fill ratio of 50%. Limiting the initial fill ratio to 41.6% provides for 20% future growth.

[15] Refer to NEC Sections 770.12 and 376.22. Section 376.22 limits wireway fill to 20%. Limiting the initial fill ratio to 16.7% provides for 20% future growth.

[16] Refer to §5.2.2.2 in TIA/EIA-569-A.

[17] Refer to §7.2.2.2 in TIA/EIA-569-A.

[18] Refer to §9.4.2.2 in TIA/EIA-569-A.

[19] Refer to §9.4.2.2 in TIA/EIA-569-A.

[20] Requirements for Protected Distribution Systems in Chapter 5 of DOE M 200.1-1 are extended to the entrance conduits.

5. PTS ductbanks must pass a comprehensive visual inspection by the PTS Site Manager before being covered.
6. Coordinate requirements with the LANL Telecommunications Group and the PTS Site Manager.

I. PTS Cables

1. LANL will install one GFE horizontal PTS cable for each terminal connection.
   a. GFE PTS horizontal cable typically consists of multiple tight-buffered multi-mode fibers; cable outside diameter is approximately 0.25 inches.
   b. *LANL will connectorize, terminate, and test the PTS horizontal cables at both ends.*
2. LANL will install GFE backbone PTS cables to interconnect the secure telecommunications rooms.
   a. CDIN fiber optic backbone cable will be UL listed as type OFNR, tight-buffered fiber-optic cable with a mixture of single-mode and multi-mode fibers. A quality assurance light test must be performed on all CDIN fiber.
   b. *LANL will connectorize, terminate, and test the PTS backbone cables at both ends*.
3. Cable installers must have BICSI Registered Installer Level 2 or equivalent certification.

J. Identification

1. Identify PTS terminal connection boxes in accordance with EIA/TIA-606; generate records acceptable to the LANL Telecommunications Group.
2. Band CDIN raceways with 3/4-inch wide red plastic tape on 3-ft centers. Start bands 2 inches from the protected outlet boxes.
3. Identify each PTS pathway and cable in accordance with EIA/TIA-606; generate records acceptable to the LANL Telecommunications Group. Use materials and installation methods described in LANL Master Specification Section 26 0553, *Identification for Electrical Systems*.

K. Telephone/FAX Communications

1. Secure communications systems shall comply with DOE M 200.1-1
2. Classified communications areas with teletype, data, and/or facsimile capabilities should normally be designed as a centralized and consolidated service area within a secured area located in close proximity to the principal users.
3. Centers that are electro-magnetically shielded shall be windowless and without skylights or roof windows; shall have column-free operating areas; and shall have clear ceiling heights of not less than 8 feet. Acoustic treatment shall be installed as required to maintain acceptable internal sound levels.
4. Telecommunications, alarm, and AIS centers shall be centralized and consolidated to, maximize the range of electrical and communication systems coverage, reduce on-site distribution of service cable and duct lengths, maximize the efficiency and effectiveness of physical protection systems and minimize operation and maintenance costs.
5. Telephone circuits shall be used for other telecommunications and alarm services to the maximum extent practicable. If separate conductors are required, they shall be routed through the main telecommunications and signal raceway systems if raceway systems are present. Separate wire-ways and cabinets shall be used only when necessary to meet security, technical, or code requirements or to achieve significant economies.
6. Cable trays that penetrate security barriers shall provide the same degree of penetration resistance as required by the site-specific security plan for the barrier through which they penetrate. This

provision applies when the opening at the point the barrier is penetrated is more than 96 square inches in area and over 6 inches in smallest dimension and is located less than:

- 18 feet above uncontrolled ground, roofs, or ledges.
- 14 feet diagonally or directly opposite windows, fire escapes, roofs, or other openings in uncontrolled buildings.
- 6 feet from uncontrolled openings in the same barrier.

7. Electric power distribution systems shall be filtered to reduce emanation of detectable electro-magnetic signals to acceptable levels as directed by the cognizant DOE telecommunications and security personnel. Installations shall comply with DOE 200.1- 1.
8. Data processing, amplifying, telecommunications, and other systems that emit electromagnetic emanations, and communications lines to remote interrogation points used to process classified data processing information, shall be protected against compromise of such data in accordance with DOE 200.1-1.
9. Telephones or public address systems in conference rooms or offices in which classified discussions at the Secret or Top Secret level occur shall comply with DOE O 6430.1A, Section 0110-99.10, Secure Conference Rooms, and Section 0110-99.11, Secure Offices, respectively.
10. Where transmissions of classified data outside security areas are involved, NSA-approved encryption shall be used.
11. Telecommunications, alarm and AIS centers and radio repeater stations shall be housed in fire-resistant structures and located outside areas subject to explosion, fire, flood, chemical fumes, excessive dust, vibration, dampness, high noise levels, and high electrical interference. Protective measures shall be implemented in all instances where these facilities cannot be located outside such areas.
12. The configuration of maintenance, operating, storage and utility areas and equipment within telecommunications, alarm, and AIS centers and radio repeater stations shall:
    - Provide adequate maintenance service access to maintain all equipment. The minimum aisle space between cabinets or rack-mounted equipment and adjacent walls shall be 3 feet. Additional clearance shall be provided for high-voltage equipment and to allow for equipment change out.
    - Consolidate related equipment and operations area.
    - Provide physical protection for equipment, operations, and storage areas.
13. Operating and equipment areas of centers and repeater stations that contain relays, switches, electronic devices, and other dust-sensitive equipment shall be designed to be relatively dust-free. To minimize the intrusion of dirt and dust into operating and equipment areas, these areas shall be windowless and without skylights or roof windows. All exterior doors shall be weather-stripped. Access to the equipment and operating areas shall be through vestibules, foyers, corridors or other buffer areas.
14. Operating areas shall be located and constructed to minimize outside noise interference and treated acoustically to maintain a low internal sound level commensurate with operating requirements.
15. Internal columns shall be avoided in areas of telecommunications, alarm, and automated information systems (AIS) centers that require shielded enclosures.

L. Protective Force Communication Requirements

1. Facilities with Protected Areas, Material Access Areas, and Vital Areas shall have two different technologies of voice communications, to link each fixed post, Central Alarm Station (CAS), Secondary Alarm Station (SAS), and protected personnel dispatch point within the facility.

2. Radio communications equipment shall remain operable in the event of a loss of primary electric power. Communications equipment shall allow rapid, reliable, and protected information exchange between on-site protective forces; between on-site protective forces and the CASs and secondary communications station; and between the CASs, secondary communications stations, and local law enforcement agencies.
3. Alternate communications capabilities shall be available immediately upon failure of the primary communications system. Channels considered critical to protective personnel communications shall have backup stations.
4. Facilities within Protected Areas, Material Access Areas, and Vital Areas shall have duress capabilities between mobile and fixed posts.
5. Interior communications and alarm systems shall be designed to use standard, commercially available equipment. The initial and projected requirements for telecommunications systems shall comply with DOE M 200.1-1. Secure communication systems, TEMPEST criteria, protected transmission systems, data communications facilities, services, and equipment shall comply with DOE M 200.1-1.
6. Systems shall remain operable in the event of loss of primary electrical power.
7. Standby or emergency power supplies for security, communications, and alarm systems shall be provided.
8. Duress alarms shall not annunciate at the post initiating the duress alarm.
9. The duress alarm for a Central Alarm Station shall annunciate at the Secondary Alarm Station or another fixed protective force post.
10. The duress alarm for the Secondary Alarm Station shall annunciate at the Central Alarm Station or another fixed post.
11. Mobile duress alarms shall annunciate at the Central Alarm Station, Secondary Alarm Station, or another fixed post.
12. Portable radios shall be capable of two-way communication on the primary security channel from within critical buildings and structures. If safety or process procedures prohibit transmission within a building or structure, an alternate means of communication shall be provided.
13. Where radio communications or control equipment requires one or more exposed antennas having no significant blast resistance, provisions shall be made to replace the antennas from within the shelter. Normally retracted "pop-up" antennas, operable from within the hardened area, shall be provided.
14. Sites selected for radio repeater stations shall comply with DOE M 200.1-1. Approval for a radio repeater station shall be obtained from DOE Headquarters, Office of Computer Services and Telecommunications Management.
15. Radio repeater stations shall be positioned on the site so as to ensure access by all-weather vehicular and personnel to the station building, the antenna(s), the standby generator plant, and fuel storage tank. The design shall minimize risk of damage to the antenna structure and supporting guy lines from vehicular traffic and provide for future expansion.
16. Radio Repeater Station exterior walls shall be windowless. Roofs shall be without skylights or roof windows. Space shall be provided for maintenance activities and storage of spare parts and tools.
17. Where antenna towers, poles, or masts are to be located off the building, interconnecting cables shall be placed underground or adequately supported by a messenger wire (or cable). The building end of the messenger wire shall not be secured to the bulkhead panel unless the panel and appurtenances are designed to support the load.
18. Antennas or reflectors, transmission lines, and other equipment to be mounted on the antenna structures, and the location, number, height, arrangement, and orientation of antenna structures shall comply with DOE 200.1-1.

M. Cyber Security— Automated Information Systems including Classified Systems

1. Systems that require protection include, but are not limited to:
    - Mainframe classified information systems, word processors, microprocessors, personal computers, programmable controllers, automated office support systems, memory typewriters, and other stand-alone or special systems that process, store, transfer, or provide access to classified information, including those classified information systems that also process store, transfer, or provide concurrent access to both classified and unclassified information.
    - Special purpose computers that perform classified functions and/or contain classified data, such as numerically controlled machines, smart switches, single-task preprogrammed controllers, programmable facsimile devices, automated testers, and digital-to-analog digital converters.
    - Networks wherein classified information is processed, stored, transferred, or accessed in one or more components of the network.
2. Secure communications systems shall comply with DOE requirements.
3. A classified AIS facility shall be located in a security area to provide adequate physical protection. It shall be secured to a level commensurate with the most highly classified material handled by the system. It shall be securely locked and alarmed when no authorized personnel are in attendance.
4. AIS centers shall be housed in fire-resistant structures and located outside areas subject to explosion, fire, flood, chemical fumes, excessive dust, vibration, dampness, high noise levels, and high electrical interference. Protective measures shall be implemented in all instances where these facilities cannot be located outside such areas.
5. AIS centers and remote interrogation points used for classified information shall be established as limited areas or be located within larger limited areas such that access is controlled will be as required by DOE.
6. When contained within a larger limited area, AIS centers and remote interrogation points used to process classified information shall have separate access controls and barriers to restrict access to classified information to those persons who require it in the performance of official duties and with the need-to-know.
7. AIS centers shall be centralized and consolidated to maximize the range of electrical and communication systems coverage, reduce on-site distribution service cable and duct lengths, maximize the efficiency and effectiveness of physical protection systems and minimize operation and maintenance costs.
8. Essential equipment shall be connected to un-interruptible power supply or to emergency power. Design shall be coordinated with the equipment system specialists and DOE security personnel. Where continuity of service is required for critical cord-connected equipment, twist-lock-type connectors shall be used.
9. Only NSA-approved cryptographic devices or protected transmission systems shall be used to protect classified communication lines that pass outside the security area of an AIS system or facility. The specific security area of a facility will be defined in the AIS protection plan.
10. Each communications link that leaves an AIS facility shall be protected commensurate with the most highly classified material that it carries and in accordance with DOE. If all communications links are not protected at the highest level of material carried by any one of them, other security measures shall be installed to preclude transmission of classified material over unprotected links.
11. Data processing, amplifying, telecommunications, and other systems that emit electromagnetic emanations, and communications lines to remote interrogation points used to process classified

data processing information, shall be protected against compromise of such data in accordance with DOE.

12. Measures shall be implemented on all new AIS equipment that processes classified material to prevent compromising emanations from such equipment and systems from being exploitable beyond the limits of effective physical control.
13. One or more of the following first two methods shall be used in conjunction with the fourth to prevent compromising emanations beyond the limits of the effective physical control zone:
14. Shielded enclosures. This may be a shielded room within which the equipment is contained or just an enclosure around the emanating equipment.
15. Equipment design. AIS equipment may be designed or modified to limit the strength of compromising signals to acceptable limits considering the control zone available. Radiation limit requirements shall be considered on a cost-effective basis for certain types of AIS equipment when being purchased or leased to process classified information.
16. Installation Criteria. The installation of AIS equipment and cabling shall comply with DOE M 200.1-1.
17. Adequate maintenance service access to maintain all equipment. The minimum aisle space between cabinets or rack-mounted equipment and adjacent walls shall be 3 feet. Additional clearance shall be provided for high-voltage equipment and to allow for equipment change.
18. Consolidate related equipment and operations areas.
19. Provide adequate fire-resistant wall separations between storage and maintenance areas and equipment and operations areas.
20. Provide structural, architectural, environmental, mechanical, and electrical features and systems that will mitigate the degree of renovation necessary to accommodate future expansion needs for five years after facilities are occupied.
21. Operations shall be located in the same or adjoining rooms. Supporting activities (storage, maintenance, power, and environmental control and scheduling, and administrative offices) shall be housed in separate rooms adjacent to the central operations area.
22. Walls around secure AIS centers shall be constructed of concrete masonry units or other materials that are not easily penetrated.

5.7 Exterior Security System Requirements (e.g., PIDAS, PIDADS)

Reserved for future use

6.0 Appendices

- Appendix A Required Security Signs and Postings
- Appendix B References